FinancialStrides

PCI Compliance Scanning

SCAN REPORT

Clone Systems, Inc.

DETAILED PCI REPORT

Audited on Mon Apr 13 2020 18:00:11

CONFIDENTIAL

ASV Scan Report Vulnerability Details

Part 1. Scan Information			
Scan Customer Company:	Clone Systems, Inc.	ASV Company:	Clone Systems, Inc.
Date scan was completed:	Mon Apr 13 2020 18:00:11	Scan expiration date:	Sun Jul 12 2020 18:00:11

Part 2. Vulnerability Details

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	53/tcp	The BIND version on the remote host has reached the end of life and should not be used anymore.	high	NOCVE	10.0	☐	☒
	Vulnerability Detection Result: The "BIND" version on the remote host has reached the end of life. CPE: cpe:/a:isc:bind:9.9.5.3 Installed version: 9.9.5.3 EOL version: 9.9 EOL date: 2018-07-31 **Impact:** An end of life version of BIND is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host. **Solution** Update the BIND version on the remote host to a still supported version. **Solution type:** VendorFix **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.			**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** BIND End of Life Detection (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.113016) **Version used:** $Revision: 11935 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:C/I:C/A:C) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.isc.org/downloads/software-support-policy/, URL:https://www.isc.org/downloads/			
38.123.140.31 demoweb.clone-systems.com	445/tcp	The Samba version on the remote host has reached the end of life and should not be used anymore.	high	NOCVE	10.0	☐	☒
	Vulnerability Detection Result: The "Samba" version on the remote host has reached the end of life. CPE: cpe:/a:samba:samba:4.1.6 Installed version: 4.1.6 Location/URL: 445/tcp EOL version: 4.1 EOL date: 2016-03-22 **Impact:** An end of life version of Samba is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host. **Solution** Update the Samba version on the remote host to a still supported version. **Solution type:** VendorFix **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.			**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba End Of Life Detection (NVT: 1.3.6.1.4.1.25623.1.0.140159) **Version used:** $Revision: 11923 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:C/I:C/A:C) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://wiki.samba.org/index.php/Samba_Release_Planning			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability	high	CVE-2015-0240	10.0	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 3.6.25 or 4.0.25 or 4.1.17, 4.2.0rc5, or later Installation path / port: 445/tcp **Impact:** An attacker can exploit this issue to execute arbitrary code with root privileges. Failed exploit attempts will cause a denial-of-service condition **Solution** Updates are available. Please see the references or vendor advisory for more information. **Solution type:** VendorFix **Affected Software/OS:** Samba 3.5.x and 3.6.x before 3.6.25, 4.0.x before 4.0.25, 4.1.x before 4.1.17, and 4.2.x before 4.2.0rc5 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The Netlogon server implementation in smbd performs a free operation on an uninitialized stack pointer, which allows remote attackers to execute arbitrary code via crafted Netlogon packets that use the ServerPasswordSet RPC API, as demonstrated by packets reaching the _netr_ServerPasswordSet function in rpc_server/netlogon/srv_netlog_nt.c.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.105231) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:C/I:C/A:C) **CVE:** CVE-2015-0240 **BID:** 72711 **CERT:** **XREF:** URL:http://www.securityfocus.com/bid/72711			
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to remote code execution vulnerability.	high	CVE-2017-7494	10.0	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.4.14 or apply patch Installation path / port: 445/tcp **Impact:** Successfully exploiting this issue will allow remote attackers to execute arbitrary code as root on an affected system. **Solution** Upgrade to Samba 4.6.4 or 4.5.10 or 4.4.14 or later. **Solution type:** VendorFix **Affected Software/OS:** All Samba Server versions 3.5.0 onwards, Samba Server versions 4.4.x before 4.4.14, Samba Server versions 4.5.x before 4.5.10, and Samba Server versions 4.6.x before 4.6.4 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to an input validation error, which allows a malicious client to upload a shared library to a writable share.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba Remote Code Execution Vulnerability (SambaCry) (NVT: 1.3.6.1.4.1.25623.1.0.811055) **Version used:** $Revision: 11888 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:C/I:C/A:C) **CVE:** CVE-2017-7494 **BID:** 98636 **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2017-7494.html, URL:http://hackaday.com/2017/05/25/linux-sambacry/, URL:http://thehackernews.com/2017/05/samba-rce-exploit.html, URL:https://github.com/omri9741/cve-2017-7494			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	22/tcp	This host is running OpenSSH and is prone to multiple vulnerabilities.	high	CVE-2015-6564, CVE-2015-6563, CVE-2015-5600	8.5	☐	☒
	Vulnerability Detection Result: Installed version: 6.6.1p1 Fixed version: 7.0 Installation path / port: 22/tcp **Impact:** Successful exploitation will allow an attacker to gain privileges, to conduct impersonation attacks, to conduct brute-force attacks or cause a denial of service. Impact Level: Application **Solution** Upgrade to OpenSSH 7.0 or later. For updates refer to http://www.openssh.com **Solution type:** VendorFix **Affected Software/OS:** OpenSSH versions before 7.0 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaws are due to: - Use-after-free vulnerability in the 'mm_answer_pam_free_ctx' function in monitor.c in sshd. - Vulnerability in 'kbdint_next_device' function in auth2-chall.c in sshd. - vulnerability in the handler for the MONITOR_REQ_PAM_FREE_CTX request.		**Vulnerability Detection Method:** Get the installed version with the help of detect NVT and check the version is vulnerable or not. **Details:** OpenSSH Multiple Vulnerabilities (NVT: 1.3.6.1.4.1.25623.1.0.806052) **Version used:** $Revision: 4336 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:C) **CVE:** CVE-2015-6564, CVE-2015-6563, CVE-2015-5600 **BID:** NOBID **CERT:** **XREF:** URL:http://seclists.org/fulldisclosure/2015/Aug/54, URL:http://openwall.com/lists/oss-security/2015/07/23/4			
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to remote code execution vulnerability.	high	CVE-2014-3560	7.9	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.1.11 Installation path / port: 445/tcp **Impact:** Successfully exploiting this issue will allow remote attackers to execute arbitrary code on the affected system. **Solution** Upgrade to Samba 4.0.21 or 4.1.11 or later. **Solution type:** VendorFix **Affected Software/OS:** Samba Server versions 4.0.x before 4.0.21 and 4.1.x before 4.1.11. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to an insufficient mechanism to avoid buffer overwriting. A malicious user can send packets that may overwrite the heap of the target nmbd NetBIOS name services daemon.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba 'nmbd' NetBIOS Name Services Daemon Remote Code Execution Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.811220) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:A/AC:M/Au:N/C:C/I:C/A:C) **CVE:** CVE-2014-3560 **BID:** 69021 **CERT:** **XREF:** URL:http://www.securitytracker.com/id/1030663, URL:http://www.samba.org/samba/security/CVE-2014-3560			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	22/tcp	This host is installed with openssh and is prone to denial of service vulnerability.	high	CVE-2016-6515	7.8	☐	☒
	Vulnerability Detection Result: Installed version: 6.6.1p1 Fixed version: 7.3 Installation path / port: 22/tcp **Impact:** Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption). Impact Level: Application **Solution** Upgrade to OpenSSH version 7.3 or later. For updates refer to http://www.openssh.com **Solution type:** VendorFix **Affected Software/OS:** OpenSSH versions before 7.3 on Linux **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to the auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication.						
	Vulnerability Detection Method: Get the installed version with the help of detect NVT and check the version is vulnerable or not. **Details:** OpenSSH 'auth_password' Denial of Service Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.809154) **Version used:** $Revision: 4336 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:C) **CVE:** CVE-2016-6515 **BID:** 92212 **CERT:** **XREF:** URL:http://www.openssh.com/txt/release-7.3, URL:http://openwall.com/lists/oss-security/2016/08/01/2						
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to remote denial of service vulnerability.	high	CVE-2015-5722	7.8	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.7-P3 **Impact:** Successful exploitation will allow remote attackers to cause denial of service. **Solution** Upgrade to ISC BIND version 9.9.7-P3 or 9.10.2-P4 or later. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.0.0 through 9.8.8 and 9.9.0 through 9.9.7-P2 and 9.10.x through 9.10.2-P3. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to an error in 'buffer.c' script in ISC BIND.						
	Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** ISC BIND 'buffer.c' Script Remote Denial of Service Vulnerability - Jan16 (NVT: 1.3.6.1.4.1.25623.1.0.807202) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:C) **CVE:** CVE-2015-5722 **BID:** 76605 **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01287						
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to denial of service vulnerability.	high	CVE-2016-2776	7.8	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.9-P3 **Impact:** Successful exploitation will allow remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query. **Solution** Upgrade to ISC BIND version 9.9.9-P3 or 9.10.4-P3 or 9.11.0rc3 or later on Linux. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to the 'buffer.c' script in named in ISC BIND does not properly construct responses.						
	Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** ISC BIND 'buffer.c' Assertion Failure Denial of Service Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.810263) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:C) **CVE:** CVE-2016-2776 **BID:** 93188 **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01419/0						

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	53/tcp	ISC BIND is prone to a denial of service vulnerability.	high	CVE-2016-2776	7.8	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.9-P3 **Impact:** An remote attacker may cause a denial of service condition. **Solution** Upgrade to 9.9.9-P3, 9.9.9-S5, 9.10.4-P3, 9.11.0rc3 or later. **Solution type:** VendorFix **Affected Software/OS:** BIND 9 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** A crafted query could crash the BIND name server daemon, leading to a denial of service. All server roles (authoritative, recursive and forwarding) in default configurations are affected.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND Denial of Service Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.106291) **Version used:** 2019-07-24T08:39:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:C) **CVE:** CVE-2016-2776 **BID:** NOBID **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01419			
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to denial of service vulnerability.	high	CVE-2015-4620	7.8	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.7-P1 **Impact:** Successful exploitation will allow attackers to cause denial of service to clients. **Solution** Upgrade to ISC BIND version 9.9.7-P1 or 9.10.2-P2 or later. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.7.x through 9.9.x before 9.9.7-P1 and 9.10.x before 9.10.2-P2 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to an error in 'name.c' script in ISC BIND when configured as a recursive resolver with DNSSEC validation.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND Denial of Service Vulnerability - Oct15 (NVT: 1.3.6.1.4.1.25623.1.0.806079) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:C) **CVE:** CVE-2015-4620 **BID:** NOBID **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01267			
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to denial of service vulnerability.	high	CVE-2014-8500	7.8	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.6-P1 **Impact:** Successful exploitation will allow attackers to cause denial of service to clients. **Solution** Upgrade to ISC BIND version 9.9.6-p1 or 9.10.1-p1 or later for branches of BIND (9.9 and 9.10). **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.0.x through 9.8.x, 9.9.0 through 9.9.6, and 9.10.0 through 9.10.1 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to ISC BIND does not handle delegation chaining properly.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND Delegation Handling Denial of Service Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.806080) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:C) **CVE:** CVE-2014-8500 **BID:** NOBID **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01216/0/			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to remote denial of service vulnerability.	high	CVE-2015-5477	7.8	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.7-P2 **Impact:** Successful exploitation will allow remote attackers to cause denial of service. **Solution** Upgrade to ISC BIND version 9.9.7-P2 or 9.10.2-P3 or later. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.1.0 through 9.9.7-P1, 9.10.0 through 9.10.2-P2. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to an error in handling TKEY queries can cause named to exit with a REQUIRE assertion failure.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND Denial of Service Vulnerability - 06 - Jan16 (NVT: 1.3.6.1.4.1.25623.1.0.807200) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:C) **CVE:** CVE-2015-5477 **BID:** 76092 **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01272				
38.123.140.31 demoweb.clone-systems.com	80/tcp	This host is running Apache HTTP Server and is prone to multiple vulnerabilities.	high	CVE-2017-7679, CVE-2017-3169, CVE-2017-3167	7.5	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.26 **Impact:** Successful exploitation will allow remote attackers to bypass authentication and perform unauthorized actions, cause a denial-of-service condition and gain access to potentially sensitive information. **Solution** Upgrade to Apache HTTP Server 2.2.33 or 2.4.26 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server 2.2.x before 2.2.33 and 2.4.x before 2.4.26 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaws exists as, - The mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header. - The mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port. - An use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Multiple Vulnerabilities June17 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.811214) **Version used:** 2019-07-05T10:41:31+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:P/A:P) **CVE:** CVE-2017-7679, CVE-2017-3169, CVE-2017-3167 **BID:** 99135, 99134 **CERT:** **XREF:** URL:http://seclists.org/oss-sec/2017/q2/509, URL:http://httpd.apache.org/security/vulnerabilities_24.html, URL:http://httpd.apache.org/security/vulnerabilities_22.html				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	22/tcp	This host is installed with openssh and is prone to multiple vulnerabilities.	high	CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10708	7.5	☐	☒
	Vulnerability Detection Result: Installed version: 6.6.1p1 Fixed version: 7.4 Installation path / port: 22/tcp **Impact:** Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, conduct a senial-of-service condition and allows remote attackers to execute arbitrary local PKCS#11 modules. **Solution** Upgrade to OpenSSH version 7.4 or later. **Solution type:** VendorFix **Affected Software/OS:** OpenSSH versions before 7.4 on Linux **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaws exists due to, - An 'authfile.c' script does not properly consider the effects of realloc on buffer contents. - The shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers. - The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used. - An untrusted search path vulnerability in ssh-agent.c in ssh-agent. - NULL pointer dereference error due to an out-of-sequence NEWKEYS message.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** OpenSSH Multiple Vulnerabilities Jan17 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.8103256) **Version used:** 2019-05-21T12:48:06+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:P/A:P) **CVE:** CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10708 **BID:** 94968, 94972, 94977, 94975 **CERT:** **XREF:** URL:https://www.openssh.com/txt/release-7.4, URL:http://www.openwall.com/lists/oss-security/2016/12/19/2, URL:http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html, URL:https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e933e6b931de1d16737			
38.123.140.31 demoweb.clone-systems.com	8082/tcp	This host is running Apache HTTP Server and is prone to multiple vulnerabilities.	high	CVE-2017-7679, CVE-2017-3169, CVE-2017-3167	7.5	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.26 **Impact:** Successful exploitation will allow remote attackers to bypass authentication and perform unauthorized actions, cause a denial-of-service condition and gain access to potentially sensitive information. **Solution** Upgrade to Apache HTTP Server 2.2.33 or 2.4.26 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server 2.2.x before 2.2.33 and 2.4.x before 2.4.26 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaws exists as, - The mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header. - The mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port. - An use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Multiple Vulnerabilities June17 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.811214) **Version used:** 2019-07-05T10:41:31+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:P/A:P) **CVE:** CVE-2017-7679, CVE-2017-3169, CVE-2017-3167 **BID:** 99135, 99134 **CERT:** **XREF:** URL:http://seclists.org/oss-sec/2017/q2/509, URL:http://httpd.apache.org/security/vulnerabilities_24.html, URL:http://httpd.apache.org/security/vulnerabilities_22.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	22/tcp	This host is installed with openssh and is prone to security bypass vulnerability.	high	CVE-2016-1908	7.5	☐	☒
	Vulnerability Detection Result: Installed version: 6.6.1p1 Fixed version: 7.2 Installation path / port: 22/tcp **Impact:** Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks. **Solution** Upgrade to OpenSSH version 7.2 or later. **Solution type:** VendorFix **Affected Software/OS:** OpenSSH versions before 7.2 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** An access flaw was discovered in OpenSSH, It did not correctly handle failures to generate authentication cookies for untrusted X11 forwarding. A malicious or compromised remote X application could possibly use this flaw to establish a trusted connection to the local X server, even if only untrusted X11 forwarding was requested.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.810769) **Version used:** 2019-05-22T12:00:57+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:P/A:P) **CVE:** CVE-2016-1908 **BID:** 84427 **CERT:** **XREF:** URL:http://openwall.com/lists/oss-security/2016/01/15/13, URL:https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4, URL:http://www.openssh.com/txt/release-7.2, URL:https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6fa0db113c71e234416c, URL:https://bugzilla.redhat.com/show_bug.cgi?id=1298741			
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to a use-after-free vulnerability.	high	CVE-2017-14746	7.5	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.5.15 Installation path / port: 445/tcp **Impact:** A malicious SMB1 request can be used to control the contents of heap memory via a deallocated heap pointer. It is possible this may be used to compromise the SMB server. **Solution** Update to Samba 4.5.15, 4.6.11, 4.7.3 or later. Workaround: Prevent SMB1 access to the server by setting the parameter: server min protocol = SMB2 to the [global] section of your smb.conf and restart smbd. This prevents a SMB1 access to the server. Note this could cause older clients to be unable to connect to the server. **Solution type:** VendorFix **Affected Software/OS:** Samba versions 4.0.0 to 4.5.14, 4.6.x prior to 4.6.11, 4.7.x prior to 4.7.3 with enabled SMBv1 support. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to a client which may use an SMB1 request to manipulate the contents of heap space.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba Server 'CVE-2017-14746' Use-after-free Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.108294) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:P/A:P) **CVE:** CVE-2017-14746 **BID:** 101907 **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2017-14746.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	22/tcp	This host is installed with openssh and is prone to privilege escalation vulnerability.	high	CVE-2015-8325	7.2	☐	☒
	Vulnerability Detection Result: Installed version: 6.6.1p1 Fixed version: 7.2p2-3 Installation path / port: 22/tcp **Impact:** Successfully exploiting this issue will allow local users to gain privileges. Impact Level: Application **Solution** Upgrade to OpenSSH version 7.2p2-3 or later. For updates refer to http://www.openssh.com **Solution type:** VendorFix **Affected Software/OS:** OpenSSH versions through 7.2p2 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to an error in 'do_setup_env function' in 'session.c' script in sshd which trigger a crafted environment for the /bin/login program when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories.						
	Vulnerability Detection Method: Get the installed version with the help of detect NVT and check the version is vulnerable or not. **Details:** OpenSSH Privilege Escalation Vulnerability - May16 (NVT: 1.3.6.1.4.1.25623.1.0.807574) **Version used:** $Revision: 4336 $ **References:** **CVSS v2 Vector:** (AV:L/AC:L/Au:N/C:C/I:C/A:C) **CVE:** CVE-2015-8325 **BID:** NOBID **CERT:** **XREF:** URL:https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html, URL:https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4e10a65c91810f88755						
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to remote denial of service vulnerability.	medium	CVE-2015-8704	6.8	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.8-P3 **Impact:** Successful exploitation will allow remote attackers to cause denial of service. Impact Level: Application **Solution** Upgrade to ISC BIND version 9.9.8-P3 or 9.10.3-P3 or 9.9.8-S4 or later. For updates refer to https://www.isc.org **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.3.0 through 9.8.8, 9.9.0 through 9.9.8-P2, 9.9.3-S1 through 9.9.8-S3, 9.10.0 through 9.10.3-P2. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to an error in 'apl_42.c' script in ISC BIND.						
	Vulnerability Detection Method: Get the installed version with the help of detect NVT and check the version is vulnerable or not. **Details:** ISC BIND Denial of Service Vulnerability - 02 - Jan16 (NVT: 1.3.6.1.4.1.25623.1.0.806996) **Version used:** $Revision: 4429 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:S/C:N/I:N/A:C) **CVE:** CVE-2015-8704 **BID:** NOBID **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01335						

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	80/tcp	The host is installed with Apache HTTP server and is prone to multiple vulnerabilities.	medium	CVE-2018-1312, CVE-2018-1283, CVE-2017-15715, CVE-2017-15710, CVE-2018-1301	6.8	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.30 Installation path / port: 80/tcp **Impact:** Successful exploitation will allow an attacker to replay HTTP requests across servers without detection, influence the user content, upload a malicious file, crash the Apache HTTP Server and perform denial of service attack. **Solution** Upgrade to version 2.4.30 or later. Please see the references for more information. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP server versions from 2.4.1 to 2.4.4, 2.4.6, 2.4.7, 2.4.9, 2.4.10, 2.4.12, 2.4.16 to 2.4.18, 2.4.20, 2.4.23, 2.4.25 to 2.4.29 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaws exists due to, - Apache HTTP Server fails to correctly generate the nonce sent to prevent reply attacks. - Misconfigured mod_session variable, HTTP_SESSION. - Apache HTTP Server fails to sanitize the expression specified in 'FilesMatch>'. - An error in Apache HTTP Server 'mod_authnz_ldap' when configured with AuthLDAPCharsetConfig. - Apache HTTP Server fails to sanitize against a specially crafted request.					
	Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.812844) **Version used:** 2019-05-03T08:55:39+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:P) **CVE:** CVE-2018-1312, CVE-2018-1283, CVE-2017-15715, CVE-2017-15710, CVE-2018-1301 **BID:** 103524, 103520, 103525, 103512, 103515 **CERT:** **XREF:** URL:https://httpd.apache.org/download.cgi, URL:https://httpd.apache.org/security/vulnerabilities_24.html					

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to badlock vulnerability.	medium	CVE-2016-2118, CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-0128	6.8	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.2.11 or 4.3.8 or 4.4.2, or later Installation path / port: 445/tcp **Impact:** Successful exploitation of this vulnerability leads to Man-in-the-middle (MITM) attacks, to causes denial of service, to spoof and to obtain sensitive session information. Impact Level: Application **Solution** Upgrade to samba version 4.2.11, or 4.3.8, or 4.4.2, or later. **Solution type:** VendorFix **Affected Software/OS:** Samba versions 3.0.x through 4.4.1 ----- NOTE: Samba versions 4.2.11, 4.3.8 are not affected ----- **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The multiple flaws are due to - The Multiple errors in DCE-RPC code. - A spoofing Vulnerability in NETLOGON. - The LDAP implementation did not enforce integrity protection for LDAP connections. - The SSL/TLS certificates are not validated in certain connections. - Not enforcing Server Message Block (SMB) signing for clients using the SMB1 protocol. - An integrity protection for IPC traffic is not enabled by default - The MS-SAMR and MS-LSAD protocol implementations mishandle DCERPC connections. - An error in the implementation of NTLMSSP authentication. -		**Vulnerability Detection Method:** Get the installed version with the help of detect NVT and check the version is vulnerable or not. **Details:** Samba Badlock Critical Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.807646) **Version used:** $Revision: 4401 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:P) **CVE:** CVE-2016-2118, CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-0128 **BID:** NOBID **CERT:** **XREF:** URL:http://badlock.org/, URL:http://thehackernews.com/2016/03/windows-samba-vulnerability.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	8082/tcp	The host is installed with Apache HTTP server and is prone to multiple vulnerabilities.	medium	CVE-2018-1312, CVE-2018-1283, CVE-2017-15715, CVE-2017-15710, CVE-2018-1301	6.8	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.30 Installation path / port: 8082/tcp **Impact:** Successful exploitation will allow an attacker to replay HTTP requests across servers without detection, influence the user content, upload a malicious file, crash the Apache HTTP Server and perform denial of service attack. **Solution** Upgrade to version 2.4.30 or later. Please see the references for more information. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP server versions from 2.4.1 to 2.4.4, 2.4.6, 2.4.7, 2.4.9, 2.4.10, 2.4.12, 2.4.16 to 2.4.18, 2.4.20, 2.4.23, 2.4.25 to 2.4.29 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaws exists due to, - Apache HTTP Server fails to correctly generate the nonce sent to prevent reply attacks. - Misconfigured mod_session variable, HTTP_SESSION. - Apache HTTP Server fails to sanitize the expression specified in 'FilesMatch>'. - An error in Apache HTTP Server 'mod_authnz_ldap' when configured with AuthLDAPCharsetConfig. - Apache HTTP Server fails to sanitize against a specially crafted request.					
	Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.812844) **Version used:** 2019-05-03T08:55:39+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:P) **CVE:** CVE-2018-1312, CVE-2018-1283, CVE-2017-15715, CVE-2017-15710, CVE-2018-1301 **BID:** 103524, 103520, 103525, 103512, 103515 **CERT:** **XREF:** URL:https://httpd.apache.org/download.cgi, URL:https://httpd.apache.org/security/vulnerabilities_24.html					

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	80/tcp	This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.	medium	CVE-2014-3523, CVE-2014-0118, CVE-2014-0226, CVE-2014-0231	6.8	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.10 **Impact:** Successful exploitation will allow a remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives. **Solution** Upgrade to version 2.4.10 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server version before 2.4.10. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaws are due to: - Vulnerability in the WinNT MPM component within the 'winnt_accept' function in server/mpm/winnt/child.c script that is triggered when the default AcceptFilter is used. - Vulnerability in the mod_deflate module that is triggered when handling highly compressed bodies. - A race condition in the mod_status module that is triggered as user-supplied input is not properly validated when handling the scoreboard. - Vulnerability in the mod_cgid module that is triggered when used to host CGI scripts that do not consume standard input.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Multiple Vulnerabilities May15 (NVT: 1.3.6.1.4.1.25623.1.0.805638) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:P) **CVE:** CVE-2014-3523, CVE-2014-0118, CVE-2014-0226, CVE-2014-0231 **BID:** 73040 **CERT:** **XREF:** URL:http://httpd.apache.org/security/vulnerabilities_24.html, URL:http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109			
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to man-in-the-middle vulnerability.	medium	CVE-2016-2119	6.8	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.2.14 Installation path / port: 445/tcp **Impact:** Successful exploitation will allow a remote attacker to bypass a client-signing protection mechanism, and consequently spoof SMB2 and SMB3 servers. Impact Level: Application **Solution** Upgrade to Samba version 4.2.14 or 4.3.11 or 4.4.5 or later. For updates refer to https://www.samba.org **Solution type:** VendorFix **Affected Software/OS:** Samba versions 4.x before 4.2.14, 4.3.x before 4.3.11, and 4.4.x before 4.4.5. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists in the way DCE/RPC connections are initiated by the user. Any authenticated DCE/RPC connection that a client initiates against the server could be use by a man-in-the middle attacker to impersonate the server by injecting the SMB2_SESSION_FLAG_IS_GUEST or SMB2_SESSION_FLAG_IS_NULL flag.		**Vulnerability Detection Method:** Get the installed version with the help of detect NVT and check the version is vulnerable or not. **Details:** Samba 'libcli/smb/smbXcli_base.c' Man In The Middle (MIMA) Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.807345) **Version used:** $Revision: 4401 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:P) **CVE:** CVE-2016-2119 **BID:** NOBID **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2016-2119.html, URL:https://access.redhat.com/security/cve/cve-2016-2119			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	8082/tcp	This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.	medium	CVE-2014-3523, CVE-2014-0118, CVE-2014-0226, CVE-2014-0231	6.8	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.10 **Impact:** Successful exploitation will allow a remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives. **Solution** Upgrade to version 2.4.10 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server version before 2.4.10. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaws are due to: - Vulnerability in the WinNT MPM component within the 'winnt_accept' function in server/mpm/winnt/child.c script that is triggered when the default AcceptFilter is used. - Vulnerability in the mod_deflate module that is triggered when handling highly compressed bodies. - A race condition in the mod_status module that is triggered as user-supplied input is not properly validated when handling the scoreboard. - Vulnerability in the mod_cgid module that is triggered when used to host CGI scripts that do not consume standard input.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Multiple Vulnerabilities May15 (NVT: 1.3.6.1.4.1.25623.1.0.805638) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:P) **CVE:** CVE-2014-3523, CVE-2014-0118, CVE-2014-0226, CVE-2014-0231 **BID:** 73040 **CERT:** **XREF:** URL:http://httpd.apache.org/security/vulnerabilities_24.html, URL:http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109			
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to a MITM authentication validation bypass vulnerability.	medium	CVE-2017-11103	6.8	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.4.15 Installation path / port: 445/tcp **Impact:** Successfully exploiting this issue will allow a MITM attacker to impersonate a trusted server and thus gain elevated access to the domain by returning malicious replication or authorization data. **Solution** Upgrade to Samba 4.6.6 or 4.5.12 or 4.4.15 or later or apply the patch from below. **Solution type:** VendorFix **Affected Software/OS:** All versions of Samba from 4.0.0 before 4.6.6 or 4.5.12 or 4.4.15. Note: All versions of Samba from 4.0.0 onwards using embedded Heimdal Kerberos. Samba binaries built against MIT Kerberos are not vulnerable. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to error in function '_krb5_extract_ticket' where the KDC-REP service name must be obtained from encrypted version stored in 'enc_part' instead of the unencrypted version stored in 'ticket'. Use of the unecrypted version provides an opportunity for successful server impersonation and other attacks.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba Man in the Middle Security Bypass Vulnerability (Heimdal) (NVT: 1.3.6.1.4.1.25623.1.0.811522) **Version used:** $Revision: 11901 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:P) **CVE:** CVE-2017-11103 **BID:** 99551 **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2017-11103.html, URL:https://www.samba.org/samba/security			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to denial-of-service vulnerability.	medium	CVE-2017-9461	6.8	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.4.10 Installation path / port: 445/tcp **Impact:** Successfully exploiting this issue will allow remote attackers to conduct a denial-of-service condition(infinite loop with high CPU usage and memory consumption). **Solution** Upgrade to Samba 4.4.10 or 4.5.6 or later. **Solution type:** VendorFix **Affected Software/OS:** Samba versions before 4.4.10 and 4.5.x before 4.5.6 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to error in smbd which enters infinite loop when trying to open an invalid symlink with O_CREAT.			**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba 'fd_open_atomic infinite loop' Denial-of-Service Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.811083) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:S/C:N/I:N/A:C) **CVE:** CVE-2017-9461 **BID:** NOBID **CERT:** **XREF:** URL:https://bugzilla.samba.org/show_bug.cgi?id=12572, URL:https://git.samba.org/?p=samba.git;a=commit;h=10c3e3923022485c720f322ca4f0aca5d7501310			
38.123.140.31 demoweb.clone-systems.com	445/tcp	Multiple Vulnerabilities in Samba 4.0 onward.	medium	CVE-2018-1050, CVE-2018-1057	6.5	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.5.16 Installation path / port: 445/tcp **Impact:** Successful exploitation would result in effects ranging from Denial of Service to Privilege Escalation, eventually allowing an attacker to gain full control over the target system. **Solution** Update to Samba version 4.5.16, 4.6.14 or 4.7.6 respectively. **Solution type:** VendorFix **Affected Software/OS:** Samba 4.x.x before 4.5.16, 4.6.x before 4.6.14 and 4.7.x before 4.7.6. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** There exist two vulnerabilities: - Samba is vulnerable to a denial of service attack when the RPC spoolss service is configured to be run as an external daemon. Missing input sanitization checks on some of the input parameters to spoolss RPC calls could cause the print spooler service to crash. - On a Samba AD DC the LDAP server in Samba incorrectly validates permissions to modify passwords over LDAP allowing authenticated users to change any other users' passwords, including administrative users and privileged service accounts (eg Domain Controllers).			**Vulnerability Detection Method:** The script checks if a vulnerable version is present on the target host. **Details:** Samba 4 Multiple Vulnerabilities (NVT: 1.3.6.1.4.1.25623.1.0.113133) **Version used:** $Revision: 12120 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:S/C:P/I:P/A:P) **CVE:** CVE-2018-1050, CVE-2018-1057 **BID:** NOBID **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2018-1050.html, URL:https://www.samba.org/samba/security/CVE-2018-1057.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	Multiple Vulnerabilities in Samba 4.0 onward.	medium	CVE-2018-1050, CVE-2018-1057	6.5	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.5.16 Installation path / port: 445/tcp **Impact:** Successful exploitation would result in effects ranging from Denial of Service to Privilege Escalation, eventually allowing an attacker to gain full control over the target system. **Solution** Update to Samba version 4.5.16, 4.6.14 or 4.7.6 respectively. **Solution type:** VendorFix **Affected Software/OS:** Samba 4.x.x before 4.5.16, 4.6.x before 4.6.14 and 4.7.x before 4.7.6. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** There exist two vulnerabilities: - Samba is vulnerable to a denial of service attack when the RPC spoolss service is configured to be run as an external daemon. Missing input sanitization checks on some of the input parameters to spoolss RPC calls could cause the print spooler service to crash. - On a Samba AD DC the LDAP server in Samba incorrectly validates permissions to modify passwords over LDAP allowing authenticated users to change any other users' passwords, including administrative users and privileged service accounts (eg Domain Controllers).		**Vulnerability Detection Method:** The script checks if a vulnerable version is present on the target host. **Details:** Samba 4 Multiple Vulnerabilities (NVT: 1.3.6.1.4.1.25623.1.0.113133) **Version used:** $Revision: 12120 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:S/C:P/I:P/A:P) **CVE:** CVE-2018-1050, CVE-2018-1057 **BID:** NOBID **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2018-1050.html, URL:https://www.samba.org/samba/security/CVE-2018-1057.html			
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to a heap based buffer overflow vulnerability.	medium	CVE-2018-10858	6.5	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.6.16 or apply patch Installation path / port: 445/tcp **Impact:** Successful exploitation will allow an attacker to conduct a denial of service attack. **Solution** Upgrade to Samba 4.6.16, 4.7.9 or 4.8.4 or later. Please see the references for more information. **Solution type:** VendorFix **Affected Software/OS:** Samba versions 3.2.0 through 4.8.3 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to insufficient input validation on client directory listing in libsmbclient.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba 'libsmbclient' Heap Buffer Overflow Vulnerability - Aug18 (NVT: 1.3.6.1.4.1.25623.1.0.813782) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:S/C:P/I:P/A:P) **CVE:** CVE-2018-10858 **BID:** NOBID **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2018-10858.html, URL:https://www.samba.org/samba/history/samba-4.6.16.html, URL:https://www.samba.org/samba/history/samba-4.7.9.html, URL:https://www.samba.org/samba/history/samba-4.8.4.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	8082/tcp	This host is running Apache HTTP Server and is prone to multiple vulnerabilities.	medium	CVE-2017-9788	6.4	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.27 **Impact:** Successful exploitation will allow remote attackers to cause the target service to crash. A remote user can obtain potentially sensitive information as well on the target system. **Solution** Upgrade to Apache HTTP Server 2.2.34 or 2.4.27 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server 2.2.x before 2.2.34 and 2.4.x before 2.4.27 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to error in Apache 'mod_auth_digest' which does not properly initialize memory used to process 'Digest' type HTTP Authorization headers.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.811237) **Version used:** $Revision: 14173 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:P) **CVE:** CVE-2017-9788 **BID:** 99569 **CERT:** **XREF:** URL:http://www.securitytracker.com/id/1038906, URL:http://httpd.apache.org/security/vulnerabilities_22.html, URL:http://httpd.apache.org/security/vulnerabilities_24.html		
38.123.140.31 demoweb.clone-systems.com	80/tcp	This host is running Apache HTTP Server and is prone to multiple vulnerabilities.	medium	CVE-2017-9788	6.4	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.27 **Impact:** Successful exploitation will allow remote attackers to cause the target service to crash. A remote user can obtain potentially sensitive information as well on the target system. **Solution** Upgrade to Apache HTTP Server 2.2.34 or 2.4.27 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server 2.2.x before 2.2.34 and 2.4.x before 2.4.27 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to error in Apache 'mod_auth_digest' which does not properly initialize memory used to process 'Digest' type HTTP Authorization headers.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.811237) **Version used:** $Revision: 14173 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:P) **CVE:** CVE-2017-9788 **BID:** 99569 **CERT:** **XREF:** URL:http://www.securitytracker.com/id/1038906, URL:http://httpd.apache.org/security/vulnerabilities_22.html, URL:http://httpd.apache.org/security/vulnerabilities_24.html		
38.123.140.31 demoweb.clone-systems.com	general/tcp	In Apache HTTP Server, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.	medium	CVE-2019-0217	6.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.39 **Solution** Update to version 2.4.39 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP server version 2.4.38 and prior. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.142220) **Version used:** 2019-04-15T07:08:44+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:S/C:P/I:P/A:P) **CVE:** CVE-2019-0217 **BID:** NOBID **CERT:** **XREF:** URL:https://httpd.apache.org/security/vulnerabilities_24.html		

<table>
<tr><th rowspan="2">Component</th><th rowspan="2">Detected Open Ports, Services/ Protocols</th><th rowspan="2">Vulnerability</th><th rowspan="2">Severity Level</th><th rowspan="2">CVE Number</th><th rowspan="2">CVSS Score</th><th colspan="2">Compliance Status</th></tr>
<tr><th>Pass</th><th>Fail</th></tr>
<tr><td rowspan="2">38.123.140.31
demoweb.clone-systems.com</td><td>445/tcp</td><td>Samba is prone to a user impersonation vulnerability.</td><td>medium</td><td>CVE-2018-16860</td><td>6.0</td><td>☐</td><td>☒</td></tr>
<tr><td colspan="2">Vulnerability Detection Result: Installed version: 4.1.6
Fixed version: 4.8.12
Installation
path / port: 445/tcp
Impact: This allows a man-in-the-middle attacker who can intercept the request to the KDC to modify the packet by replacing the user name (principal) in the request with any desired user name (principal) that exists in the KDC and replace the checksum protecting that name with a CRC32 checksum (which requires no prior knowledge to compute). This would allow a S4U2Self ticket requested on behalf of user name (principal) user@EXAMPLE.COM to any service to be changed to a S4U2Self ticket with a user name (principal) of Administrator@EXAMPLE.COM. This ticket would then contain the PAC of the modified user name (principal).
Solution
Update to version 4.8.12, 4.9.8, 4.10.3 or later.
Solution type: VendorFix Affected Software/OS: All Samba versions since Samba 4.0.
Detection Reliability: Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.
Vulnerability Insight: S4U2Self is an extension to Kerberos used in Active Directory to allow a service to request a kerberos ticket to itself from the Kerberos Key Distribution Center (KDC) for a non-Kerberos authenticated user (principal in Kerboros parlance). This is useful to allow internal code paths to be standardized around Kerberos.
S4U2Proxy (constrained-delegation) is an extension of this mechanism allowing this impersonation to a second service over the network. It allows a privileged server that obtained a S4U2Self ticket to itself to then assert the identity of that principal to a second service and present itself as that principal to get services from the second service.
There is a flaw in Samba's AD DC in the Heimdal KDC. When the Heimdal KDC checks the checksum that is placed on the S4U2Self packet by the server to protect the requested principal against modification, it does not confirm that the checksum algorithm that protects the user name (principal) in the request is keyed.</td><td colspan="5">Vulnerability Detection Method: Checks if a vulnerable version is present on the target host.
Details: Samba AD DC Principal Modification Vulnerability (CVE-2018-16860) (NVT: 1.3.6.1.4.1.25623.1.0.108575)
Version used: 2019-08-14T06:47:48+0000
References:
CVSS v2 Vector: (AV:N/AC:M/Au:S/C:P/I:P/A:P)
CVE: CVE-2018-16860
BID: NOBID
CERT:
XREF: URL:https://www.samba.org/samba/security/CVE-2018-16860.html</td></tr>
<tr><td rowspan="2">38.123.140.31
demoweb.clone-systems.com</td><td>general/tcp</td><td>In Apache HTTP Server, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.</td><td>medium</td><td>CVE-2019-0217</td><td>6.0</td><td>☐</td><td>☒</td></tr>
<tr><td colspan="2">Vulnerability Detection Result: Installed version: 2.4.7
Fixed version: 2.4.39
Solution
Update to version 2.4.39 or later.
Solution type: VendorFix Affected Software/OS: Apache HTTP server version 2.4.38 and prior.
Detection Reliability: Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.</td><td colspan="5">Vulnerability Detection Method: Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.142220)
Version used: 2019-04-15T07:08:44+0000
References:
CVSS v2 Vector: (AV:N/AC:M/Au:S/C:P/I:P/A:P)
CVE: CVE-2019-0217
BID: NOBID
CERT:
XREF: URL:https://httpd.apache.org/security/vulnerabilities_24.html</td></tr>
</table>

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to MitM vulnerability.	medium	CVE-2017-12150	5.8	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.4.16, or 4.5.14, or 4.6.8 Installation path / port: 445/tcp **Impact:** Successful exploitation will allow a remote attacker to read and/or alter the content of the connection. **Solution** Upgrade to Samba 4.6.8, 4.5.14 or 4.4.16 **Solution type:** VendorFix **Affected Software/OS:** Samba versions 3.0.25 to 4.6.7 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to there are several code paths where the code doesn't enforce SMB signing.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba Server 'SMB 1/2/3' MitM Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.811907) **Version used:** $Revision: 11983 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:N) **CVE:** CVE-2017-12150 **BID:** 100918 **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2017-12150.html		
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to MitM vulnerability.	medium	CVE-2017-12151	5.8	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.4.16, or 4.5.14, or 4.6.8 Installation path / port: 445/tcp **Impact:** Successful exploitation will allow a remote attacker to read and/or alter the content of the connection. **Solution** Upgrade to Samba 4.6.8, 4.5.14 or 4.4.16 **Solution type:** VendorFix **Affected Software/OS:** Samba versions 4.1.0 to 4.6.7 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** A connection actually made use of the SMB3 encryption, any redirected connection would lose the requirement for encryption and also the requirement for signing.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba Server 'SMB3' MitM Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.811906) **Version used:** $Revision: 11983 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:N) **CVE:** CVE-2017-12151 **BID:** 100917 **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2017-12151.html		
38.123.140.31 demoweb.clone-systems.com	22/tcp	openssh xauth command injection may lead to forced-command and /bin/false bypass	medium	CVE-2016-3115	5.5	☐	☒
	Vulnerability Detection Result: Installed version: 6.6.1p1 Fixed version: 7.2p2 Installation path / port: 22/tcp **Impact:** By injecting xauth commands one gains limited* read/write arbitrary files, information leakage or xauth-connect capabilities. **Solution** Upgrade to OpenSSH version 7.2p2 or later. For updates refer to http://www.openssh.com **Solution type:** VendorFix **Affected Software/OS:** OpenSSH versions before 7.2p2 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie. The newline acts as a command separator to the xauth binary. This attack requires the server to have 'X11Forwarding yes' enabled. Disabling it, mitigates this vector.				**Vulnerability Detection Method:** Get the installed version with the help of detect NVT and check the version is vulnerable or not. **Details:** OpenSSH = 7.2p1 - Xauth Injection (NVT: 1.3.6.1.4.1.25623.1.0.105581) **Version used:** $Revision: 2970 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:S/C:P/I:P/A:N) **CVE:** CVE-2016-3115 **BID:** NOBID **CERT:** **XREF:** URL:http://www.openssh.com/txt/release-7.2p2		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	Samba is prone to a path/symlink traversal vulnerability.	medium	CVE-2019-3880	5.5	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.8.11 Installation path / port: 445/tcp **Solution** Update to version 4.8.11, 4.9.6, 4.10.2 or later. **Solution type:** VendorFix **Affected Software/OS:** Samba 3.2.0 and later. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share.			**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba Path/Symlink Traversal Vulnerability (CVE-2019-3880) (NVT: 1.3.6.1.4.1.25623.1.0.142391) **Version used:** 2019-05-09T14:21:05+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:S/C:N/I:P/A:P) **CVE:** CVE-2019-3880 **BID:** NOBID **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2019-3880.html			
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to remote denial of service vulnerability.	medium	CVE-2015-1349	5.4	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.10.1-P2 **Impact:** Successful exploitation will allow remote attackers to cause denial of service. **Solution** Upgrade to ISC BIND version 9.10.1-P2 or later. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.7.0 through 9.10.1-P1. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to an error in Trust Anchor Management that can cause named to crash.			**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND Denial of Service Vulnerability - 05 - Jan16 (NVT: 1.3.6.1.4.1.25623.1.0.806999) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:H/Au:N/C:N/I:N/A:C) **CVE:** CVE-2015-1349 **BID:** 72673 **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01235			
38.123.140.31 demoweb.clone-systems.com	8082/tcp	This host is installed with Apache HTTP Server and is prone to man-in-the-middle attack vulnerability.	medium	CVE-2016-5387	5.1	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.24 **Impact:** Successful exploitation will allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted proxy header in an HTTP request. **Solution** Upgrade to version 2.4.24, or 2.2.32, or newer. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server through 2.4.23 on Linux - --- NOTE: Apache HTTP Server 2.2.32 is not vulnerable - --- **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to 'CGI Servlet' does not protect applications from the presence of untrusted client data in the 'HTTP_PROXY' environment variable.			**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Man-in-the-Middle attack Vulnerability - July16 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.808632) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:H/Au:N/C:P/I:P/A:P) **CVE:** CVE-2016-5387 **BID:** 91816 **CERT:** **XREF:** URL:https://www.apache.org/security/asf-httpoxy-response.txt			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	80/tcp	This host is installed with Apache HTTP Server and is prone to man-in-the-middle attack vulnerability.	medium	CVE-2016-5387	5.1	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.24 **Impact:** Successful exploitation will allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted proxy header in an HTTP request. **Solution** Upgrade to version 2.4.24, or 2.2.32, or newer. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server through 2.4.23 on Linux - --- NOTE: Apache HTTP Server 2.2.32 is not vulnerable - --- **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to 'CGI Servlet' does not protect applications from the presence of untrusted client data in the 'HTTP_PROXY' environment variable.						
						Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Man-in-the-Middle attack Vulnerability - July16 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.808632) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:H/Au:N/C:P/I:P/A:P) **CVE:** CVE-2016-5387 **BID:** 91816 **CERT:** **XREF:** URL:https://www.apache.org/security/asf-httpoxy-response.txt	
38.123.140.31 demoweb.clone-systems.com	22/tcp	This host is installed with openssh and is prone to user enumeration vulnerability.	medium	CVE-2018-15919	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 6.6.1p1 Fixed version: None Installation path / port: 22/tcp **Impact:** Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks. **Solution** No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. **Solution type:** WillNotFix **Affected Software/OS:** OpenSSH version 5.9 to 7.8 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.						
						Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.813888) **Version used:** 2019-09-26T09:12:46+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:N) **CVE:** CVE-2018-15919 **BID:** NOBID **CERT:** **XREF:** URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163, URL:https://seclists.org/oss-sec/2018/q3/180	

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	8082/tcp	This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.	medium	CVE-2015-0228	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.13 **Impact:** Successful exploitation will allow a remote attackers to cause a denial of service via some crafted dimension. **Solution** Upgrade to version 2.4.13 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server versions through 2.4.12. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Flaw is due to vulnerability in lua_websocket_read function in lua_request.c in the mod_lua module.			**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Mod_Lua Denial of service Vulnerability -01 May15 (NVT: 1.3.6.1.4.1.25623.1.0.805616) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2015-0228 **BID:** 73041 **CERT:** **XREF:** URL:https://bugs.mageia.org/show_bug.cgi?id=15428, URL:http://svn.apache.org/repos/asf/httpd/httpd/branches/2.4.x/CHANGES			
38.123.140.31 demoweb.clone-systems.com	80/tcp	This host is running Apache HTTP Server and is prone to multiple vulnerabilities.	medium	CVE-2015-3185, CVE-2015-3183	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.14 **Impact:** Successful exploitation will allow remote attackers to bypass intended access restrictions in opportunistic circumstances and to cause cache poisoning or credential hijacking if an intermediary proxy is in use. Impact Level: Application **Solution** Upgrade to version 2.4.14 or later, For updates refer to http://www.apache.org **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server version 2.4.x before 2.4.14 on linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaws are due to: - an error in 'ap_some_auth_required' function in 'server/request.c' script which does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting. - an error in chunked transfer coding implementation.			**Vulnerability Detection Method:** Get the installed version with the help of detect NVT and check the version is vulnerable or not. **Details:** Apache HTTP Server Multiple Vulnerabilities August15 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.806018) **Version used:** $Revision: 4161 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:P/A:N) **CVE:** CVE-2015-3185, CVE-2015-3183 **BID:** 75965, 75963 **CERT:** **XREF:** URL:http://www.apache.org/dist/httpd/CHANGES_2.4, URL:http://httpd.apache.org/security/vulnerabilities_24.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to remote denial of service vulnerability.	medium	CVE-2015-8000	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.8-P2 **Impact:** Successful exploitation will allow remote attackers to cause denial of service. **Solution** Upgrade to ISC BIND version 9.9.8-P2 or 9.10.3-P2 or later. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.0.x through 9.9.8, 9.10.0 through 9.10.3. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to an error in 'db.c' script in ISC BIND.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND Denial of Service Vulnerability - 03 - Jan16 (NVT: 1.3.6.1.4.1.25623.1.0.806997) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2015-8000 **BID:** 79349 **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01317				
38.123.140.31 demoweb.clone-systems.com	80/tcp	This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.	medium	CVE-2015-0228	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.13 **Impact:** Successful exploitation will allow a remote attackers to cause a denial of service via some crafted dimension. **Solution** Upgrade to version 2.4.13 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server versions through 2.4.12. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Flaw is due to vulnerability in lua_websocket_read function in lua_request.c in the mod_lua module.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Mod_Lua Denial of service Vulnerability -01 May15 (NVT: 1.3.6.1.4.1.25623.1.0.805616) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2015-0228 **BID:** 73041 **CERT:** **XREF:** URL:https://bugs.mageia.org/show_bug.cgi?id=15428, URL:http://svn.apache.org/repos/asf/httpd/httpd/branches/2.4.x/CHANGES				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	8082/tcp	Apache HTTP server allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed.	medium	CVE-2017-9798	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.28 **Impact:** The successful exploitation allows the attacker to read chunks of the host's memory. **Solution** Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references. As a workaround the usage of .htaccess should be disabled competely via the 'AllowOverride None' directive within the webservers configuration. Furthermore all Limit> statements within the webserver configuration needs to be verified for invalid HTTP methods. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server 2.2.x versions up to 2.2.34 and 2.4.x below 2.4.28. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Optionsbleed is a use after free error in Apache HTTP server that causes a corrupted Allow header to be constructed in response to HTTP OPTIONS requests. This can leak pieces of arbitrary memory from the server process that may contain secrets. The memory pieces change after multiple requests, so for a vulnerable host an arbitrary number of memory chunks can be leaked. The bug appears if a webmaster tries to use the 'Limit' directive with an invalid HTTP method. Example .htaccess: Limit abcxyz> /Limit>		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) (NVT: 1.3.6.1.4.1.25623.1.0.108252) **Version used:** $Revision: 11983 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:N) **CVE:** CVE-2017-9798 **BID:** 100872 **CERT:** **XREF:** URL:http://openwall.com/lists/oss-security/2017/09/18/2, URL:https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTIONS-method-can-leak-Apaches-server-memory.html, URL:http://www.securityfocus.com/bid/100872, URL:https://archive.apache.org/dist/httpd/patches/apply_to_2.2.34/, URL:https://www.apache.org/dist/httpd/CHANGES_2.4.28			
38.123.140.31 demoweb.clone-systems.com	22/tcp	This host is installed with openssh and is prone to denial of service vulnerability.	medium	CVE-2016-1907	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 6.6.1p1 Fixed version: 7.1p2 Installation path / port: 22/tcp **Impact:** Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read and application crash). Impact Level: Application **Solution** Upgrade to OpenSSH version 7.1p2 or later. For updates refer to http://www.openssh.com **Solution type:** VendorFix **Affected Software/OS:** OpenSSH versions before 7.1p2 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to an error in 'ssh_packet_read_poll2' function within 'packet.c' script.		**Vulnerability Detection Method:** Get the installed version with the help of detect NVT and check the version is vulnerable or not. **Details:** OpenSSH Denial of Service Vulnerability - Jan16 (NVT: 1.3.6.1.4.1.25623.1.0.806671) **Version used:** $Revision: 4336 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2016-1907 **BID:** NOBID **CERT:** **XREF:** URL:http://www.openssh.com/txt/release-7.1p2, URL:https://anongit.mindrot.org/openssh.git/commit/?id=2fecfd486bdba9f51b3a789277bb0733ca36e1c0			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	8082/tcp	The host is installed with Apache HTTP server and is prone to a denial of service vulnerability.	medium	CVE-2018-1303	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.30 Installation path / port: 8082/tcp **Impact:** Successful exploitation will allow an attacker to crash the Apache HTTP Server resulting in denial of service condition. **Solution** Upgrade to version 2.4.30 or later. Please see the references for more information. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP server versions 2.4.6, 2.4.7, 2.4.9, 2.4.10, 2.4.12, 2.4.16 through 2.4.18, 2.4.20, 2.4.23, and 2.4.25 through 2.4.29 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists as the Apache HTTP Server fails to sanitize against a specially crafted HTTP request header.						
						Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.812849) **Version used:** 2019-05-03T08:55:39+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2018-1303 **BID:** 103522 **CERT:** **XREF:** URL:https://httpd.apache.org/download.cgi, URL:https://httpd.apache.org/security/vulnerabilities_24.html		
38.123.140.31 demoweb.clone-systems.com	53/tcp	ISC BIND is prone to a denial of service vulnerability.	medium	CVE-2016-8864	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.9-P4 **Impact:** An remote attacker may cause a denial of service condition. **Solution** Upgrade to 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, 9.11.0-P1 or later. **Solution type:** VendorFix **Affected Software/OS:** BIND 9 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** A defect in BIND's handling of responses containing a DNAME answer can cause a resolver to exit after encountering an assertion failure in db.c or resolver.c						
						Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** ISC BIND Denial of Service Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.106366) **Version used:** 2019-07-24T08:39:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2016-8864 **BID:** NOBID **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01434		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	80/tcp	The host is installed with Apache HTTP server and is prone to a denial of service vulnerability.	medium	CVE-2018-1303	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.30 Installation path / port: 80/tcp **Impact:** Successful exploitation will allow an attacker to crash the Apache HTTP Server resulting in denial of service condition. **Solution** Upgrade to version 2.4.30 or later. Please see the references for more information. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP server versions 2.4.6, 2.4.7, 2.4.9, 2.4.10, 2.4.12, 2.4.16 through 2.4.18, 2.4.20, 2.4.23, and 2.4.25 through 2.4.29 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists as the Apache HTTP Server fails to sanitize against a specially crafted HTTP request header.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.812849) **Version used:** 2019-05-03T08:55:39+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2018-1303 **BID:** 103522 **CERT:** **XREF:** URL:https://httpd.apache.org/download.cgi, URL:https://httpd.apache.org/security/vulnerabilities_24.html		
38.123.140.31 demoweb.clone-systems.com	993/tcp	The service is using a SSL/TLS certificate from a known untrusted certificate authority. An attacker could use this for MitM attacks, accessing sensible data and other attacks.	medium	NOCVE	5.0	☐	☒
	Vulnerability Detection Result: The certificate of the remote service is signed by the following untrusted Certificate Authority: Issuer: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server serial ....: 00CC6C568D704F8BBE valid from : 2016-08-09 13:18:58 UTC valid until: 2026-08-09 13:18:58 UTC fingerprint (SHA-1): 84C192E09BD30A3A0707042BB2181A731AFF09BE fingerprint (SHA-256): 45B822C7CCD2315D9B09BDF9F6E296315052A42057EFE51872FA7E6BDDEE1FBA **Solution** Replace the SSL/TLS certificate with one signed by a trusted certificate authority. **Solution type:** Mitigation **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerability.				**Vulnerability Detection Method:** The script reads the certificate used by the target host and checks if it was signed by an untrusted certificate authority. **Details:** SSL/TLS: Untrusted Certificate Authorities (NVT: 1.3.6.1.4.1.25623.1.0.113054) **Version used:** $Revision: 11874 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:P/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	3306/tcp	A MySQL Database server is listening on this port.	medium	NOCVE	5.0	☐	☒
	Vulnerability Detection Result: Mysql Database is listening to port: 3306 **Impact:** Database servers contain sensitive information and should not be accessible from the internet. **Solution** Please setup strict firewall rules protecting the database from being accessible from the internet. **Solution type:** Mitigation **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** Database Server Available (NVT: 1.3.6.1.4.1.25623.1.0.300004) **Version used:** $Revision: 1002 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	995/tcp	The service is using a SSL/TLS certificate from a known untrusted certificate authority. An attacker could use this for MitM attacks, accessing sensible data and other attacks.	medium	NOCVE	5.0	☐	☒
	Vulnerability Detection Result: The certificate of the remote service is signed by the following untrusted Certificate Authority: Issuer: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server serial ....: 00CC6C568D704F8BBE valid from : 2016-08-09 13:18:58 UTC valid until: 2026-08-09 13:18:58 UTC fingerprint (SHA-1): 84C192E09BD30A3A0707042BB2181A731AFF09BE fingerprint (SHA-256): 45B822C7CCD2315D9B09BDF9F6E296315052A42057EFE51872FA7E6BDDEE1FBA **Solution** Replace the SSL/TLS certificate with one signed by a trusted certificate authority. **Solution type:** Mitigation **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerability.		**Vulnerability Detection Method:** The script reads the certificate used by the target host and checks if it was signed by an untrusted certificate authority. **Details:** SSL/TLS: Untrusted Certificate Authorities (NVT: 1.3.6.1.4.1.25623.1.0.113054) **Version used:** $Revision: 11874 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:P/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	general/tcp	In Apache HTTP Server mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.	medium	CVE-2018-17199	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.38 **Solution** Update to version 2.4.38 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP server version 2.4.37 and prior. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server 2.4.38 mod_session_cookie Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.141964) **Version used:** $Revision: 13750 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:P/A:N) **CVE:** CVE-2018-17199 **BID:** NOBID **CERT:** **XREF:** URL:https://httpd.apache.org/security/vulnerabilities_24.html			
38.123.140.31 demoweb.clone-systems.com	80/tcp	Apache HTTP server allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed.	medium	CVE-2017-9798	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.28 **Impact:** The successful exploitation allows the attacker to read chunks of the host's memory. **Solution** Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references. As a workaround the usage of .htaccess should be disabled competely via the 'AllowOverride None' directive within the webservers configuration. Furthermore all Limit> statements within the webserver configuration needs to be verified for invalid HTTP methods. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server 2.2.x versions up to 2.2.34 and 2.4.x below 2.4.28. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Optionsbleed is a use after free error in Apache HTTP server that causes a corrupted Allow header to be constructed in response to HTTP OPTIONS requests. This can leak pieces of arbitrary memory from the server process that may contain secrets. The memory pieces change after multiple requests, so for a vulnerable host an arbitrary number of memory chunks can be leaked. The bug appears if a webmaster tries to use the 'Limit' directive with an invalid HTTP method. Example .htaccess: Limit abcxyz> /Limit>		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) (NVT: 1.3.6.1.4.1.25623.1.0.108252) **Version used:** $Revision: 11983 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:N) **CVE:** CVE-2017-9798 **BID:** 100872 **CERT:** **XREF:** URL:http://openwall.com/lists/oss-security/2017/09/18/2, URL:https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTIONS-method-can-leak-Apaches-server-memory.html, URL:http://www.securityfocus.com/bid/100872, URL:https://archive.apache.org/dist/httpd/patches/apply_to_2.2.34/, URL:https://www.apache.org/dist/httpd/CHANGES_2.4.28			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	22/tcp	This host is installed with openssh and is prone to user enumeration vulnerability.	medium	CVE-2018-15473	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 6.6.1p1 Fixed version: 7.8 Installation path / port: 22/tcp **Impact:** Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server. **Solution** Update to version 7.8 or later. **Solution type:** VendorFix **Affected Software/OS:** OpenSSH versions 7.7 and prior on Linux **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c			**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** OpenSSH User Enumeration Vulnerability-Aug18 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.813864) **Version used:** 2019-05-23T14:08:05+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:N) **CVE:** CVE-2018-15473 **BID:** NOBID **CERT:** **XREF:** URL:https://0day.city/cve-2018-15473.html, URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0			
38.123.140.31 demoweb.clone-systems.com	general/tcp	When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.	medium	CVE-2019-0220	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.39 **Solution** Update to version 2.4.39 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP server version 2.4.38 and prior. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.			**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server 2.4.39 URL Normalization Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.142228) **Version used:** 2019-06-17T06:50:08+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:N) **CVE:** CVE-2019-0220 **BID:** NOBID **CERT:** **XREF:** URL:https://httpd.apache.org/security/vulnerabilities_24.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	general/tcp	When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.	medium	CVE-2019-0220	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.39 **Solution** Update to version 2.4.39 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP server version 2.4.38 and prior. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server 2.4.39 URL Normalization Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.142228) **Version used:** 2019-06-17T06:50:08+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:N) **CVE:** CVE-2019-0220 **BID:** NOBID **CERT:** **XREF:** URL:https://httpd.apache.org/security/vulnerabilities_24.html			
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to denial of service vulnerability.	medium	CVE-2016-9131	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.9-P5 **Impact:** Successful exploitation will allow remote attackers to cause a denial of service (assertion failure and daemon exit) via crafted data. **Solution** Upgrade to ISC BIND version 9.9.9-P5 or 9.10.4-P5 or 9.11.0-P2 or 9.9.9-S7 or later on Linux. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.4.0 through 9.6-ESV-R11-W1, 9.8.5 through 9.8.8, 9.9.3 through 9.9.9-P4, 9.9.9-S1 through 9.9.9-S6, 9.10.0 through 9.10.4-P4 and 9.11.0 through 9.11.0-P1 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to an error in the processing of a malformed query response received in response to a RTYPE ANY query.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND RTYPE ANY Query Denial of Service Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.810287) **Version used:** 2019-07-24T08:39:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2016-9131 **BID:** 95386 **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01439/0			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to a denial of service vulnerability.	medium	CVE-2018-5740	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.13-P1 **Impact:** Successful exploitation will allow remote attackers to cause a denial of service (assertion failure). **Solution** Upgrade to ISC BIND version 9.9.13-P1 or 9.10.8-P1 or 9.11.4-P1 or 9.12.2-P1 or 9.11.3-S3 or later. Please see the references for more information. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.7.0 through 9.8.8, 9.9.0 through 9.9.13, 9.10.0 through 9.10.8, 9.11.0 through 9.11.4, 9.12.0 through 9.12.2 and 9.13.0 through 9.13.2. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to a defect in the feature 'deny-answer-aliases' which leads to assertion failure in 'name.c'.						
	Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** ISC BIND 'deny-answer-aliases' Denial of Service Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.813750) **Version used:** 2019-07-24T08:39:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2018-5740 **BID:** NOBID **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01639/0, URL:https://kb.isc.org/article/AA-01646/81/BIND-9.11.3-S3-Release-Notes.html, URL:https://kb.isc.org/article/AA-01645/81/BIND-9.12.2-P1-Release-Notes.html, URL:https://kb.isc.org/article/AA-01644/81/BIND-9.11.4-P1-Release-Notes.html, URL:https://kb.isc.org/article/AA-01643/81/BIND-9.10.8-P1-Release-Notes.html, URL:https://kb.isc.org/article/AA-01642/81/BIND-9.9.13-P1-Release-Notes.html					
38.123.140.31 demoweb.clone-systems.com	25/tcp	The Mailserver on this host answers to VRFY and/or EXPN requests.	medium	NOCVE	5.0	☐	☒
	Vulnerability Detection Result: 'VRFY root' produces the following answer: 252 2.0.0 root **Solution** Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP. **Solution type:** Workaround **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerability. **Vulnerability Insight:** VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.						
	Details: Check if Mailserver answer to VRFY and EXPN requests (NVT: 1.3.6.1.4.1.25623.1.0.100072) **Version used:** $Revision: 13470 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:http://cr.yp.to/smtp/vrfy.html					
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to a heap memory information leak.	medium	CVE-2017-15275	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.5.15 Installation path / port: 445/tcp **Impact:** There is no known vulnerability associated with this error, but uncleared heap memory may contain previously used data that may help an attacker compromise the server via other methods. Uncleared heap memory may potentially contain password hashes or other high-value data. **Solution** Update to Samba 4.5.15, 4.6.11, 4.7.3 or later. **Solution type:** VendorFix **Affected Software/OS:** Samba versions 3.6.0 to 4.5.14, 4.6.x prior to 4.6.11, 4.7.x prior to 4.7.3. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to the server which may return the contents of heap allocated memory to the client.						
	Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** Samba Server 'CVE-2017-15275' Heap Memory Information Leak (NVT: 1.3.6.1.4.1.25623.1.0.108295) **Version used:** $Revision: 11983 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:N) **CVE:** CVE-2017-15275 **BID:** 101908 **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2017-15275.html					

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	8082/tcp	This host is running Apache HTTP Server and is prone multiple vulnerabilities.	medium	CVE-2016-8743	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.25 **Impact:** Successful exploitation will allow remote attackers to conduct request smuggling, response splitting and cache pollution attacks. **Solution** Upgrade to Apache HTTP Server 2.2.32 or 2.4.25 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server 2.2.x before 2.2.32 and 2.3.x through 2.4.24 prior to 2.4.25 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaw exists as application accepted a broad pattern of unusual whitespace patterns from the user-agent, including bare CR, FF, VTAB in parsing the request line and request header lines, as well as HTAB in parsing the request line. Any bare CR present in request lines was treated as whitespace and remained in the request field member 'the_request', while a bare CR in the request header field name would be honored as whitespace, and a bare CR in the request header field value was retained the input headers array. Implied additional whitespace was accepted in the request line and prior to the ':' delimiter of any request header lines.						
						Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities (NVT: 1.3.6.1.4.1.25623.1.0.812033) **Version used:** $Revision: 11983 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:P/A:N) **CVE:** CVE-2016-8743 **BID:** 95077 **CERT:** **XREF:** URL:https://httpd.apache.org/security/vulnerabilities_22.html, URL:https://httpd.apache.org/security/vulnerabilities_24.html	
38.123.140.31 demoweb.clone-systems.com	8082/tcp	This host is running Apache HTTP Server and is prone to multiple vulnerabilities.	medium	CVE-2015-3185, CVE-2015-3183	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.14 **Impact:** Successful exploitation will allow remote attackers to bypass intended access restrictions in opportunistic circumstances and to cause cache poisoning or credential hijacking if an intermediary proxy is in use. Impact Level: Application **Solution** Upgrade to version 2.4.14 or later, For updates refer to http://www.apache.org **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server version 2.4.x before 2.4.14 on linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaws are due to: - an error in 'ap_some_auth_required' function in 'server/request.c' script which does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting. - an error in chunked transfer coding implementation.						
						Vulnerability Detection Method: Get the installed version with the help of detect NVT and check the version is vulnerable or not. **Details:** Apache HTTP Server Multiple Vulnerabilities August15 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.806018) **Version used:** $Revision: 4161 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:P/A:N) **CVE:** CVE-2015-3185, CVE-2015-3183 **BID:** 75965, 75963 **CERT:** **XREF:** URL:http://www.apache.org/dist/httpd/CHANGES_2.4, URL:http://httpd.apache.org/security/vulnerabilities_24.html	

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	25/tcp	The Mailserver on this host answers to VRFY and/or EXPN requests.	medium	NOCVE	5.0	☐	☒
	Vulnerability Detection Result: 'VRFY root' produces the following answer: 252 2.0.0 root **Solution** Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP. **Solution type:** Workaround **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerability. **Vulnerability Insight:** VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.		**Details:** Check if Mailserver answer to VRFY and EXPN requests (NVT: 1.3.6.1.4.1.25623.1.0.100072) **Version used:** $Revision: 13470 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:http://cr.yp.to/smtp/vrfy.html			
38.123.140.31 demoweb.clone-systems.com	53/tcp	ISC BIND is prone to multiple vulnerabilities.	medium	CVE-2018-5744, CVE-2018-5745, CVE-2019-6465	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.11.5-P4 **Solution** Update to version 9.11.5-S5, 9.11.5-P4, 9.12.3-P4 or later. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.9.0-9.10.8-P1, 9.11.0-9.11.5-P2, 9.12.0-9.12.3-P2 and 9.9.3-S1-9.11.5-S3. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** ISC BIND is prone to multiple vulnerabilities: - A specially crafted packet can cause named to leak memory (CVE-2018-5744) - An assertion failure can occur if a trust anchor rolls over to an unsupported key algorithm when using managed-keys (CVE-2018-5745) - Zone transfer controls for writable DLZ zones were not effective (CVE-2019-6465)		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND Multiple Vulnerabilities - Feb19 (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.142033) **Version used:** 2019-11-08T08:01:14+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2018-5744, CVE-2018-5745, CVE-2019-6465 **BID:** NOBID **CERT:** **XREF:** URL:https://kb.isc.org/docs/cve-2018-5744, URL:https://kb.isc.org/docs/cve-2018-5745, URL:https://kb.isc.org/docs/cve-2019-6465			
38.123.140.31 demoweb.clone-systems.com	8082/tcp	This host is running Apache HTTP Server and is prone to denial-of-service vulnerability	medium	CVE-2016-2161	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.25 **Impact:** Successful exploitation will allow remote attackers to cause a denial-of-service condition. **Solution** Upgrade to Apache HTTP Server 2.4.25 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server versions 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2 and 2.4.1 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to insufficient handling of malicious input to 'mod_auth_digest'.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server 'mod_auth_digest' DoS Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.812067) **Version used:** 2019-05-17T13:14:58+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2016-2161 **BID:** 95076 **CERT:** **XREF:** URL:https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2016-2161			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	22/tcp	This host is installed with openssh and is prone to security bypass vulnerability.	medium	CVE-2017-15906	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 6.6.1p1 Fixed version: 7.6 Installation path / port: 22/tcp **Impact:** Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks. **Solution** Upgrade to OpenSSH version 7.6 or later. **Solution type:** VendorFix **Affected Software/OS:** OpenSSH versions before 7.6 on Linux **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.			**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.812051) **Version used:** 2019-05-23T14:08:05+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:P/A:N) **CVE:** CVE-2017-15906 **BID:** 101552 **CERT:** **XREF:** URL:https://www.openssh.com/txt/release-7.6, URL:https://github.com/openbsd/src/commit/a6981567e8e			
38.123.140.31 demoweb.clone-systems.com	110/tcp	The service is using a SSL/TLS certificate from a known untrusted certificate authority. An attacker could use this for MitM attacks, accessing sensible data and other attacks.	medium	NOCVE	5.0	☐	☒
	Vulnerability Detection Result: The certificate of the remote service is signed by the following untrusted Certificate Authority: Issuer: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server serial ....: 00CC6C568D704F8BBE valid from : 2016-08-09 13:18:58 UTC valid until: 2026-08-09 13:18:58 UTC fingerprint (SHA-1): 84C192E09BD30A3A0707042BB2181A731AFF09BE fingerprint (SHA-256): 45B822C7CCD2315D9B09BDF9F6E296315052A42057EFE51872FA7E6BDDEE1FBA **Solution** Replace the SSL/TLS certificate with one signed by a trusted certificate authority. **Solution type:** Mitigation **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerability.			**Vulnerability Detection Method:** The script reads the certificate used by the target host and checks if it was signed by an untrusted certificate authority. **Details:** SSL/TLS: Untrusted Certificate Authorities (NVT: 1.3.6.1.4.1.25623.1.0.113054) **Version used:** $Revision: 11874 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:P/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	80/tcp	This host is running Apache HTTP Server and is prone to denial-of-service vulnerability	medium	CVE-2016-2161	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.25 **Impact:** Successful exploitation will allow remote attackers to cause a denial-of-service condition. **Solution** Upgrade to Apache HTTP Server 2.4.25 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server versions 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2 and 2.4.1 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to insufficient handling of malicious input to 'mod_auth_digest'.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server 'mod_auth_digest' DoS Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.812067) **Version used:** 2019-05-17T13:14:58+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2016-2161 **BID:** 95076 **CERT:** **XREF:** URL:https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2016-2161		
38.123.140.31 demoweb.clone-systems.com	80/tcp	This host is running Apache HTTP Server and is prone multiple vulnerabilities.	medium	CVE-2016-8743	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.25 **Impact:** Successful exploitation will allow remote attackers to conduct request smuggling, response splitting and cache pollution attacks. **Solution** Upgrade to Apache HTTP Server 2.2.32 or 2.4.25 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server 2.2.x before 2.2.32 and 2.3.x through 2.4.24 prior to 2.4.25 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaw exists as application accepted a broad pattern of unusual whitespace patterns from the user-agent, including bare CR, FF, VTAB in parsing the request line and request header lines, as well as HTAB in parsing the request line. Any bare CR present in request lines was treated as whitespace and remained in the request field member 'the_request', while a bare CR in the request header field name would be honored as whitespace, and a bare CR in the request header field value was retained the input headers array. Implied additional whitespace was accepted in the request line and prior to the ':' delimiter of any request header lines.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities (NVT: 1.3.6.1.4.1.25623.1.0.812033) **Version used:** $Revision: 11983 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:P/A:N) **CVE:** CVE-2016-8743 **BID:** 95077 **CERT:** **XREF:** URL:https://httpd.apache.org/security/vulnerabilities_22.html, URL:https://httpd.apache.org/security/vulnerabilities_24.html		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	general/tcp	In Apache HTTP Server mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.	medium	CVE-2018-17199	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.38 **Solution** Update to version 2.4.38 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP server version 2.4.37 and prior. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server 2.4.38 mod_session_cookie Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.141964) **Version used:** $Revision: 13750 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:P/A:N) **CVE:** CVE-2018-17199 **BID:** NOBID **CERT:** **XREF:** URL:https://httpd.apache.org/security/vulnerabilities_24.html				
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to denial of service vulnerability.	medium	CVE-2016-9444	5.0	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.9-P5 **Impact:** Successful exploitation will allow remote attackers to cause a denial of service (assertion failure and daemon exit) via crafted data. **Solution** Upgrade to ISC BIND version 9.9.9-P5 or 9.10.4-P5 or 9.11.0-P2 or 9.9.9-S7 or later on Linux. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND 9.6-ESV-R9 through 9.6-ESV-R11-W1, 9.8.5 through 9.8.8, 9.9.3 through 9.9.9-P4, 9.9.9-S1 through 9.9.9-S6, 9.10.0 through 9.10.4-P4 and 9.11.0 through 9.11.0-P1 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to an error in the processing of an unusually-formed answer containing a DS resource record received in response to a query.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND Unusual DS Record Response Denial of Service Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.810284) **Version used:** 2019-07-24T08:39:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2016-9444 **BID:** 95393 **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01441/0				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	143/tcp	The service is using a SSL/TLS certificate from a known untrusted certificate authority. An attacker could use this for MitM attacks, accessing sensible data and other attacks.	medium	NOCVE	5.0	☐	☒
	Vulnerability Detection Result: The certificate of the remote service is signed by the following untrusted Certificate Authority: Issuer: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server serial ....: 00CC6C568D704F8BBE valid from : 2016-08-09 13:18:58 UTC valid until: 2026-08-09 13:18:58 UTC fingerprint (SHA-1): 84C192E09BD30A3A0707042BB2181A731AFF09BE fingerprint (SHA-256): 45B822C7CCD2315D9B09BDF9F6E296315052A42057EFE51872FA7E6BDDEE1FBA **Solution** Replace the SSL/TLS certificate with one signed by a trusted certificate authority. **Solution type:** Mitigation **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerability.					
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to denial of service vulnerability.	medium	CVE-2016-0771	4.9	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.1.23 Installation path / port: 445/tcp **Impact:** Successful exploitation will allow a remote attacker to cause denial of service. Impact Level: Application **Solution** Upgrade to Samba 4.1.23 or 4.2.9 or 4.3.6 or 4.4.0rc4 later. For updates refer to https://www.samba.org/ **Solution type:** VendorFix **Affected Software/OS:** Samba versions 4.x before 4.1.23, 4.2.x before 4.2.9, 4.3.x before 4.3.6 and 4.4.x before 4.4.0rc4. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exist due to an error in AD DC configuration in the internal DNS server.					

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to memory information leak vulnerability.	medium	CVE-2017-12163	4.8	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.4.16 Installation path / port: 445/tcp **Impact:** Successful exploitation will allow a client with write access to a share can cause server memory contents to be written into a file or printer. **Solution** Upgrade to Samba 4.6.8, 4.5.14 and 4.4.16 or later. **Solution type:** VendorFix **Affected Software/OS:** Samba versions before 4.4.16, 4.5.0 before 4.5.14, and 4.6.0 before 4.6.8. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** A server memory information leak bug over SMB1 if a client can write data to a share. Some SMB1 write requests were not correctly range checked to ensure the client had sent enough data to fulfill the write.						
38.123.140.31 demoweb.clone-systems.com	22/tcp	The OpenSSH client code between 5.4 and 7.1 contains experimental support for resuming SSH-connections (roaming). The matching server code has never been shipped, but the client code was enabled by default and could be tricked by a malicious server into leaking client memory to the server, including private client user keys. The authentication of the server host key prevents exploitation by a man-in-the-middle, so this information leak is restricted to connections to malicious or compromised servers.	medium	CVE-2016-0777, CVE-2016-0778	4.6	☐	☒
	Vulnerability Detection Result: Installed version: 6.6.1p1 Fixed version: 7.1p2 Installation path / port: 22/tcp **Solution** Update to 7.1p or newer. **Solution type:** VendorFix **Affected Software/OS:** OpenSSH >= 5.4 7.1p2 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.						

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	110/tcp	It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.	medium	NOCVE	4.3	☐	☒
	Vulnerability Detection Result: In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) NVT. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The SSLv2 and SSLv3 protocols containing known cryptographic flaws.		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.111012) **Version used:** $Revision: 4686 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/			
38.123.140.31 demoweb.clone-systems.com	25/tcp	This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.	medium	CVE-2015-0204	4.3	☐	☒
	Vulnerability Detection Result: *1 (Click here to access the vulnerability details) **Impact:** Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream. **Solution** - Remove support for 'RSA_EXPORT' cipher suites from the service. - If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later. **Solution type:** VendorFix **Affected Software/OS:** - Hosts accepting 'RSA_EXPORT' cipher suites - OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.		**Vulnerability Detection Method:** Check previous collected cipher suites saved in the KB. **Details:** SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK) (NVT: 1.3.6.1.4.1.25623.1.0.805142) **Version used:** 2019-07-05T09:29:25+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:N/I:P/A:N) **CVE:** CVE-2015-0204 **BID:** 71936 **CERT:** **XREF:** URL:https://freakattack.com, URL:http://secpod.org/blog/?p=3818, URL:http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	53/tcp	A flaw was found in the way BIND handled TSIG authentication for dynamic updates. A remote attacker able to communicate with an authoritative BIND server could use this flaw to manipulate the contents of a zone, by forging a valid TSIG or SIG(0) signature for a dynamic update request.	medium	CVE-2017-3143	4.3	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.10-P2 **Solution** Update to version 9.9.10-P2, 9.10.5-P2, 9.11.1-P2, 9.9.10-S3, 9.10.5-S3 or later. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.4.0-9.8.8, 9.9.0-9.9.10-P1, 9.10.0-9.10.5-P1, 9.11.0-9.11.1-P1, 9.9.3-S1-9.9.10-S2 and 9.10.5-S1-9.10.5-S2 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND Security Bypass Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.106937) **Version used:** 2019-07-24T08:39:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:N/I:P/A:N) **CVE:** CVE-2017-3143 **BID:** NOBID **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01503/0			
38.123.140.31 demoweb.clone-systems.com	80/tcp	This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.	medium	CVE-2014-8109	4.3	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.12 **Impact:** Successful exploitation will allow a remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives. **Solution** Upgrade to version 2.4.12 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server version 2.3.x through 2.4.10. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Flaw is due to a vulnerability in LuaAuthzProvider that is triggered if a user-supplied LUA script is supplied more than once with different arguments.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Mod_Lua Denial of service Vulnerability May15 (NVT: 1.3.6.1.4.1.25623.1.0.805637) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:N/I:P/A:N) **CVE:** CVE-2014-8109 **BID:** 73040 **CERT:** **XREF:** URL:http://httpd.apache.org/security/vulnerabilities_24.html, URL:http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109			
38.123.140.31 demoweb.clone-systems.com	8082/tcp	This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.	medium	CVE-2014-8109	4.3	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.12 **Impact:** Successful exploitation will allow a remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives. **Solution** Upgrade to version 2.4.12 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server version 2.3.x through 2.4.10. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Flaw is due to a vulnerability in LuaAuthzProvider that is triggered if a user-supplied LUA script is supplied more than once with different arguments.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Mod_Lua Denial of service Vulnerability May15 (NVT: 1.3.6.1.4.1.25623.1.0.805637) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:N/I:P/A:N) **CVE:** CVE-2014-8109 **BID:** 73040 **CERT:** **XREF:** URL:http://httpd.apache.org/security/vulnerabilities_24.html, URL:http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	8082/tcp	This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.	medium	CVE-2014-0117	4.3	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.10 **Impact:** Successful exploitation will allow a remote attackers to cause a denial of service via a crafted HTTP Connection header when a reverse proxy is enabled. **Solution** Upgrade to version 2.4.10 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server version 2.4.6 through 2.4.9. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Flaw is due to vulnerability in mod_proxy module in the Apache HTTP Server.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Mod_Cache Denial of service Vulnerability -01 May15 (NVT: 1.3.6.1.4.1.25623.1.0.805635) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:N/I:N/A:P) **CVE:** CVE-2014-0117 **BID:** 68740 **CERT:** **XREF:** URL:http://zerodayinitiative.com/advisories/ZDI-14-239/, URL:http://httpd.apache.org/security/vulnerabilities_24.html			
38.123.140.31 demoweb.clone-systems.com	80/tcp	This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.	medium	CVE-2014-0117	4.3	☐	☒
	Vulnerability Detection Result: Installed version: 2.4.7 Fixed version: 2.4.10 **Impact:** Successful exploitation will allow a remote attackers to cause a denial of service via a crafted HTTP Connection header when a reverse proxy is enabled. **Solution** Upgrade to version 2.4.10 or later. **Solution type:** VendorFix **Affected Software/OS:** Apache HTTP Server version 2.4.6 through 2.4.9. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Flaw is due to vulnerability in mod_proxy module in the Apache HTTP Server.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Apache HTTP Server Mod_Cache Denial of service Vulnerability -01 May15 (NVT: 1.3.6.1.4.1.25623.1.0.805635) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:N/I:N/A:P) **CVE:** CVE-2014-0117 **BID:** 68740 **CERT:** **XREF:** URL:http://zerodayinitiative.com/advisories/ZDI-14-239/, URL:http://httpd.apache.org/security/vulnerabilities_24.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	25/tcp	This host is prone to an information disclosure vulnerability.	medium	CVE-2014-3566	4.3	☐	☒
	Impact: Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application **Solution** Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+ **Solution type:** Mitigation **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code					**Vulnerability Detection Method:** Evaluate previous collected information about this service. **Details:** SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) (NVT: 1.3.6.1.4.1.25623.1.0.802087) **Version used:** $Revision: 4749 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2014-3566 **BID:** 70574 **CERT:** **XREF:** URL:https://www.openssl.org/~bodo/ssl-poodle.pdf, URL:https://www.imperialviolet.org/2014/10/14/poodle.html, URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html, URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html			
38.123.140.31 demoweb.clone-systems.com	110/tcp	This host is prone to an information disclosure vulnerability.	medium	CVE-2014-3566	4.3	☐	☒
	Impact: Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application **Solution** Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+ **Solution type:** Mitigation **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code					**Vulnerability Detection Method:** Evaluate previous collected information about this service. **Details:** SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) (NVT: 1.3.6.1.4.1.25623.1.0.802087) **Version used:** $Revision: 4749 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2014-3566 **BID:** 70574 **CERT:** **XREF:** URL:https://www.openssl.org/~bodo/ssl-poodle.pdf, URL:https://www.imperialviolet.org/2014/10/14/poodle.html, URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html, URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	143/tcp	This host is prone to an information disclosure vulnerability.	medium	CVE-2014-3566	4.3	☐	☒
	Impact: Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application **Solution** Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+ **Solution type:** Mitigation **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code					**Vulnerability Detection Method:** Evaluate previous collected information about this service. **Details:** SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) (NVT: 1.3.6.1.4.1.25623.1.0.802087) **Version used:** $Revision: 4749 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2014-3566 **BID:** 70574 **CERT:** **XREF:** URL:https://www.openssl.org/~bodo/ssl-poodle.pdf, URL:https://www.imperialviolet.org/2014/10/14/poodle.html, URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html, URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html				
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to denial of service vulnerability.	medium	CVE-2017-3135	4.3	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.9-P6 **Impact:** Successful exploitation will allow remote attackers to cause an INSIST assertion failure (and subsequent abort) or an attempt to read through a NULL pointer. On most platforms a NULL pointer read leads to a segmentation fault (SEGFAULT), which causes the process to be terminated. **Solution** Upgrade to ISC BIND version 9.9.9-P6 or 9.10.4-P6 or 9.11.0-P3 or 9.9.9-S8 or later. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.8.8, 9.9.3-S1 through 9.9.9-S7, 9.9.3 through 9.9.9-P5, 9.9.10b1, 9.10.0 through 9.10.4-P5, 9.10.5b1, 9.11.0 through 9.11.0-P2 and 9.11.1b1 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to using both DNS64 and RPZ to rewrite query responses, query processing can resume in an inconsistent state.					**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND DNS64 and RPZ Denial of Service Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.810547) **Version used:** 2019-07-24T08:39:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:N/I:N/A:P) **CVE:** CVE-2017-3135 **BID:** 96150 **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01453				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	993/tcp	This host is prone to an information disclosure vulnerability.	medium	CVE-2014-3566	4.3	☐	☒
	Impact: Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application **Solution** Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+ **Solution type:** Mitigation **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code					**Vulnerability Detection Method:** Evaluate previous collected information about this service. **Details:** SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) (NVT: 1.3.6.1.4.1.25623.1.0.802087) **Version used:** $Revision: 4749 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2014-3566 **BID:** 70574 **CERT:** **XREF:** URL:https://www.openssl.org/~bodo/ssl-poodle.pdf, URL:https://www.imperialviolet.org/2014/10/14/poodle.html, URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html, URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html			
38.123.140.31 demoweb.clone-systems.com	995/tcp	This host is prone to an information disclosure vulnerability.	medium	CVE-2014-3566	4.3	☐	☒
	Impact: Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application **Solution** Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+ **Solution type:** Mitigation **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code					**Vulnerability Detection Method:** Evaluate previous collected information about this service. **Details:** SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) (NVT: 1.3.6.1.4.1.25623.1.0.802087) **Version used:** $Revision: 4749 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2014-3566 **BID:** 70574 **CERT:** **XREF:** URL:https://www.openssl.org/~bodo/ssl-poodle.pdf, URL:https://www.imperialviolet.org/2014/10/14/poodle.html, URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html, URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	110/tcp	This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.	medium	CVE-2013-2566, CVE-2015-4000	4.3	☐	☒
	Vulnerability Detection Result: *2 (Click here to access the vulnerability details) **Solution** The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task. **Solution type:** Mitigation **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566). - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000). - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong		**Details:** SSL/TLS: Report Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103440) **Version used:** $Revision: 4863 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2013-2566, CVE-2015-4000 **BID:** NOBID **CERT:** **XREF:** URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/			
38.123.140.31 demoweb.clone-systems.com	143/tcp	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	medium	CVE-2016-0800, CVE-2014-3566	4.3	☐	☒
	Vulnerability Detection Result: TLS version 1.0 was detected. This version was released in 1999, it is known to be vulnerable to numerous attacks and should not be used in your environment. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 and TLSv1.0 and/or TLSv1.1 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The TLSv1.0 and TLSv1.1 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.300008) **Version used:** $Revision: 1020 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2016-0800, CVE-2014-3566 **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/, URL:https://drownattack.com/, URL:https://www.imperialviolet.org/2014/10/14/poodle.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	143/tcp	This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.	medium	CVE-2013-2566, CVE-2015-4000	4.3	☐	☒
	Vulnerability Detection Result: *3 (Click here to access the vulnerability details) **Solution** The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task. **Solution type:** Mitigation **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566). - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000). - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong				**Details:** SSL/TLS: Report Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103440) **Version used:** $Revision: 4863 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2013-2566, CVE-2015-4000 **BID:** NOBID **CERT:** **XREF:** URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/		
38.123.140.31 demoweb.clone-systems.com	110/tcp	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	medium	CVE-2016-0800, CVE-2014-3566	4.3	☐	☒
	Vulnerability Detection Result: TLS version 1.0 was detected. This version was released in 1999, it is known to be vulnerable to numerous attacks and should not be used in your environment. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 and TLSv1.0 and/or TLSv1.1 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The TLSv1.0 and TLSv1.1 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)				**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.300008) **Version used:** $Revision: 1020 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2016-0800, CVE-2014-3566 **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/, URL:https://drownattack.com/, URL:https://www.imperialviolet.org/2014/10/14/poodle.html		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	993/tcp	This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.	medium	CVE-2013-2566, CVE-2015-4000	4.3	☐	☒
	Vulnerability Detection Result: *4 (Click here to access the vulnerability details) **Solution** The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task. **Solution type:** Mitigation **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566). - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000). - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong						
38.123.140.31 demoweb.clone-systems.com	53/tcp	ISC BIND is prone to a denial of service vulnerability due to ineffective simultaneous TCP client limiting.	medium	CVE-2018-5743	4.3	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.11.6-P1 **Impact:** By exploiting the failure to limit simultaneous TCP connections, an attacker can deliberately exhaust the pool of file descriptors available to named, potentially affecting network connections and the management of files such as log files or zone journal files. In cases where the named process is not limited by OS-enforced per-process limits, this could additionally potentially lead to exhaustion of all available free file descriptors on that system. **Solution** Update to version 9.11.6-P1, 9.12.4-P1, 9.14.1, 9.11.5-S6, 9.11.6-S1 or later. **Solution type:** VendorFix **Affected Software/OS:** BIND 9.9.0 to 9.10.8-P1, 9.11.0 to 9.11.6, 9.12.0 to 9.12.4, 9.14.0. BIND 9 Supported Preview Edition versions 9.9.3-S1 to 9.11.5-S3, and 9.11.5-S5. Versions 9.13.0 to 9.13.7 of the 9.13 development branch. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** By design, BIND is intended to limit the number of TCP clients that can be connected at any given time. The number of allowed connections is a tunable parameter which, if unset, defaults to a conservative value for most servers. Unfortunately, the code which was intended to limit the number of simultaneous connections contains an error which can be exploited to grow the number of simultaneous connections beyond this limit.						

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	25/tcp	This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.	medium	CVE-2015-4000	4.3	☐	☒
	Vulnerability Detection Result: 'DHE_EXPORT' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_RC4_40_MD5 'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_RC4_40_MD5 'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_RC4_40_MD5 'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_RC4_40_MD5 **Impact:** Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application **Solution** - Remove support for 'DHE_EXPORT' cipher suites from the service - If running OpenSSL updateto version 1.0.2b or 1.0.1n or later, For updates refer to https://www.openssl.org **Solution type:** VendorFix **Affected Software/OS:** - Hosts accepting 'DHE_EXPORT' cipher suites - OpenSSL version before 1.0.2b and 1.0.1n **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.		**Vulnerability Detection Method:** Check previous collected cipher suites saved in the KB. **Details:** SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam) (NVT: 1.3.6.1.4.1.25623.1.0.805188) **Version used:** $Revision: 4781 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:N/I:P/A:N) **CVE:** CVE-2015-4000 **BID:** 74733 **CERT:** **XREF:** URL:https://weakdh.org, URL:https://weakdh.org/imperfect-forward-secrecy.pdf, URL:http://openwall.com/lists/oss-security/2015/05/20/8, URL:https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained, URL:https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes			
38.123.140.31 demoweb.clone-systems.com	995/tcp	This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.	medium	CVE-2013-2566, CVE-2015-4000	4.3	☐	☒
	Vulnerability Detection Result: *5 (Click here to access the vulnerability details) **Solution** The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task. **Solution type:** Mitigation **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566). - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000). - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong		**Details:** SSL/TLS: Report Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103440) **Version used:** $Revision: 4863 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2013-2566, CVE-2015-4000 **BID:** NOBID **CERT:** **XREF:** URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	22/tcp	This host is running OpenSSH and is prone to security bypass vulnerability.	medium	CVE-2015-5352	4.3	☐	☒
	Vulnerability Detection Result: Installed version: 6.6.1p1 Fixed version: 6.9 Installation path / port: 22/tcp **Impact:** Successful exploitation will allow remote attackers to bypass intended access restrictions. Impact Level: Application **Solution** Upgrade to OpenSSH version 6.9 or later. For updates refer to http://www.openssh.com **Solution type:** VendorFix **Affected Software/OS:** OpenSSH versions before 6.9 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to the refusal deadline was not checked within the x11_open_helper function.		**Vulnerability Detection Method:** Get the installed version with the help of detect NVT and check the version is vulnerable or not. **Details:** OpenSSH Security Bypass Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.806049) **Version used:** $Revision: 4336 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:N/I:P/A:N) **CVE:** CVE-2015-5352 **BID:** NOBID **CERT:** **XREF:** URL:http://openwall.com/lists/oss-security/2015/07/01/10			
38.123.140.31 demoweb.clone-systems.com	995/tcp	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	medium	CVE-2016-0800, CVE-2014-3566	4.3	☐	☒
	Vulnerability Detection Result: TLS version 1.0 was detected. This version was released in 1999, it is known to be vulnerable to numerous attacks and should not be used in your environment. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 and TLSv1.0 and/or TLSv1.1 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The TLSv1.0 and TLSv1.1 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.300008) **Version used:** $Revision: 1020 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2016-0800, CVE-2014-3566 **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/, URL:https://drownattack.com/, URL:https://www.imperialviolet.org/2014/10/14/poodle.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	25/tcp	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	medium	CVE-2016-0800, CVE-2014-3566	4.3	☐	☒
	Vulnerability Detection Result: TLS version 1.0 was detected. This version was released in 1999, it is known to be vulnerable to numerous attacks and should not be used in your environment. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 and TLSv1.0 and/or TLSv1.1 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The TLSv1.0 and TLSv1.1 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.300008) **Version used:** $Revision: 1020 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2016-0800, CVE-2014-3566 **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/, URL:https://drownattack.com/, URL:https://www.imperialviolet.org/2014/10/14/poodle.html			
38.123.140.31 demoweb.clone-systems.com	993/tcp	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	medium	CVE-2016-0800, CVE-2014-3566	4.3	☐	☒
	Vulnerability Detection Result: TLS version 1.0 was detected. This version was released in 1999, it is known to be vulnerable to numerous attacks and should not be used in your environment. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 and TLSv1.0 and/or TLSv1.1 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The TLSv1.0 and TLSv1.1 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.300008) **Version used:** $Revision: 1020 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2016-0800, CVE-2014-3566 **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/, URL:https://drownattack.com/, URL:https://www.imperialviolet.org/2014/10/14/poodle.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to denial of service vulnerability.	medium	CVE-2016-2775	4.3	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.9-P2 **Impact:** Successful exploitation will allow remote attackers to cause denial of service. **Solution** Upgrade to ISC BIND version 9.9.9-P2 or 9.10.4-P2 or 9.11.0b2 or later. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND versions 9.0.x through 9.9.9-P1, 9.10.0 through 9.10.4-P1, 9.11.0a3 through 9.11.0b1. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw is due to an error in the BIND implementation of the lightweight resolver protocol which use alternate method to do name resolution.					**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND 'lightweight resolver protocol' Denial of Service Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.808751) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:N/I:N/A:P) **CVE:** CVE-2016-2775 **BID:** 92037 **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01393/74/CVE-2016-2775		
38.123.140.31 demoweb.clone-systems.com	53/tcp	The host is installed with ISC BIND and is prone to denial of service vulnerability.	medium	CVE-2017-3136	4.3	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.9-P8 **Impact:** Successful exploitation will allow remote attackers to cause denial-of-service against a server. **Solution** Upgrade to ISC BIND version 9.9.9-P8 or 9.9.10rc3 or 9.10.5rc3 or 9.11.1rc3 or 9.9.9-S10 or 9.10.4-P8 or 9.11.0-P5 or later on Linux. **Solution type:** VendorFix **Affected Software/OS:** ISC BIND 9.8.0 through 9.8.8-P1, 9.9.0 through 9.9.9-P6, 9.9.10b1 through 9.9.10rc1, 9.10.0 through 9.10.4-P6, 9.10.5b1 through 9.10.5rc1, 9.11.0 through 9.11.0-P3, 9.11.1b1 through 9.11.1rc1, 9.9.3-S1 through 9.9.9-S8 on Linux. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to improper handling of queries when server is configured to use DNS64 and if the option 'break-dnssec yes' is in use.					**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND DNS64 Denial of Service Vulnerability (Linux) (NVT: 1.3.6.1.4.1.25623.1.0.810976) **Version used:** 2019-07-24T08:39:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:N/I:N/A:P) **CVE:** CVE-2017-3136 **BID:** 97653 **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01465/74/CVE-2017-3136		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	22/tcp	The remote SSH server is configured to allow weak encryption algorithms.	medium	NOCVE	4.3	☐	☒

Vulnerability Detection Result: The following weak client-to-server encryption algorithms are supported by the remote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The following weak server-to-client encryption algorithms are supported by the remote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
Solution
Disable the weak encryption algorithms.
Solution type: Mitigation **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response shows the likely presence of the vulnerable application or of the vulnerability. "Likely" means that only rare circumstances are possible where the detection would be wrong.
Vulnerability Insight: The `arcfour` cipher is the Arcfour stream cipher with 128-bit keys.
The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems
with weak keys, and should not be used anymore.
The `none` algorithm specifies that no encryption is to be done.
Note that this method provides no confidentiality protection, and it
is NOT RECOMMENDED to use it.
A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method: Check if remote ssh service supports Arcfour, none or CBC ciphers.
Details: SSH Weak Encryption Algorithms Supported (NVT: 1.3.6.1.4.1.25623.1.0.105611)
Version used: $Revision: 4490 $
References:
CVSS v2 Vector: (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVE: NOCVE
BID: NOBID
CERT:
XREF: URL:https://tools.ietf.org/html/rfc4253#section-6.3, URL:https://www.kb.cert.org/vuls/id/958563

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	53/tcp	ISC BIND is prone to a denial of service vulnerability.	medium	CVE-2016-2775	4.3	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: 9.9.9-P2 **Impact:** An remote attacker may cause a denial of service condition. **Solution** Upgrade to 9.9.9-P1, 9.10.4-P1, 9.11.0b1 or later. **Solution type:** VendorFix **Affected Software/OS:** BIND 9 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The lwresd component in BIND (which is not enabled by default) could crash while processing an overlong request name. This could lead to a denial of service.		**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** ISC BIND lwresd Denial of Service Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.106292) **Version used:** 2019-07-24T08:39:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:N/I:N/A:P) **CVE:** CVE-2016-2775 **BID:** NOBID **CERT:** **XREF:** URL:https://kb.isc.org/article/AA-01393				
38.123.140.31 demoweb.clone-systems.com	995/tcp	It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.	medium	NOCVE	4.3	☐	☒
	Vulnerability Detection Result: In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) NVT. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The SSLv2 and SSLv3 protocols containing known cryptographic flaws.		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.111012) **Version used:** $Revision: 4686 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	993/tcp	It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.	medium	NOCVE	4.3	☐	☒
	Vulnerability Detection Result: In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) NVT. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The SSLv2 and SSLv3 protocols containing known cryptographic flaws.		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.111012) **Version used:** $Revision: 4686 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/			
38.123.140.31 demoweb.clone-systems.com	143/tcp	It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.	medium	NOCVE	4.3	☐	☒
	Vulnerability Detection Result: In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) NVT. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The SSLv2 and SSLv3 protocols containing known cryptographic flaws.		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.111012) **Version used:** $Revision: 4686 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	25/tcp	It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.	medium	NOCVE	4.3	☐	☒
	Vulnerability Detection Result: In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) NVT. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The SSLv2 and SSLv3 protocols containing known cryptographic flaws.				**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.111012) **Version used:** $Revision: 4686 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/			
38.123.140.31 demoweb.clone-systems.com	143/tcp	The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size 2048).	medium	NOCVE	4.0	☐	☒
	Vulnerability Detection Result: Server Temporary Key Size: 1024 bits **Impact:** An attacker might be able to decrypt the SSL/TLS communication offline. **Solution** Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html) **Solution type:** Workaround **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.				**Vulnerability Detection Method:** Checks the DHE temporary public key size. **Details:** SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.106223) **Version used:** $Revision: 4739 $ **References:** **CVSS v2 Vector:** (AV:N/AC:H/Au:N/C:P/I:P/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://weakdh.org/, URL:https://weakdh.org/sysadmin.html			
38.123.140.31 demoweb.clone-systems.com	993/tcp	The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size 2048).	medium	NOCVE	4.0	☐	☒
	Vulnerability Detection Result: Server Temporary Key Size: 1024 bits **Impact:** An attacker might be able to decrypt the SSL/TLS communication offline. **Solution** Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html) **Solution type:** Workaround **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.				**Vulnerability Detection Method:** Checks the DHE temporary public key size. **Details:** SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.106223) **Version used:** $Revision: 4739 $ **References:** **CVSS v2 Vector:** (AV:N/AC:H/Au:N/C:P/I:P/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://weakdh.org/, URL:https://weakdh.org/sysadmin.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	53/tcp	ISC BIND is prone to a denial of service vulnerability.	medium	CVE-2016-6170	4.0	☐	☒
	Vulnerability Detection Result: Installed version: 9.9.5.3 Fixed version: Workaround **Impact:** An authenticated remote attacker may cause a denial of service condition. **Solution** As a workaround operators of servers which accept untrusted zone data can mitigate their risk by operating an intermediary server whose role it is to receive zone data and then (if successful) re-distribute it to client-facing servers. Successful exploitation of the attack against the intermediary server may still occur but denial of service against the client-facing servers is significantly more difficult to achieve in this scenario. **Solution type:** Workaround **Affected Software/OS:** Version = 9.10.4-P1 **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Primary DNS servers may cause a denial of service (secondary DNS server crash) via a large AXFR response, and possibly allows IXFR servers to cause a denial of service (IXFR client crash) via a large IXFR response and allows remote authenticated users to cause a denial of service (primary DNS server crash) via a large UPDATE message						
						Vulnerability Detection Method: Checks the version. **Details:** ISC BIND AXFR Response Denial of Service Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.106118) **Version used:** $Revision: 4446 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:S/C:N/I:N/A:P) **CVE:** CVE-2016-6170 **BID:** NOBID **CERT:** **XREF:** URL:http://www.openwall.com/lists/oss-security/2016/07/06/3, URL:https://lists.dns-oarc.net/pipermail/dns-operations/2016-July/015058.html	
38.123.140.31 demoweb.clone-systems.com	445/tcp	Samba is prone to multiple vulnerabilities.	medium	CVE-2018-14629, CVE-2018-16851	4.0	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.7.12 Installation path / port: 445/tcp **Solution** Update to version 4.7.12, 4.8.7, 4.9.3 or later. **Solution type:** VendorFix **Affected Software/OS:** Samba version 4.x.x. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Samba is prone to multiple vulnerabilities: - CNAME loops can cause DNS server crashes, and CNAMEs can be added by unprivileged users. (CVE-2018-14629) - A user able to read more than 256MB of LDAP entries can crash the Samba AD DC's LDAP server. (CVE-2018-16851)						
						Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** Samba 4.x Multiple DoS Vulnerabilities (NVT: 1.3.6.1.4.1.25623.1.0.141732) **Version used:** $Revision: 13517 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:S/C:N/I:N/A:P) **CVE:** CVE-2018-14629, CVE-2018-16851 **BID:** NOBID **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2018-14629.html, URL:https://www.samba.org/samba/security/CVE-2018-16851.html	

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to an information disclosure vulnerability.	medium	CVE-2018-10919	4.0	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.6.16 or apply patch Installation path / port: 445/tcp **Impact:** Successful exploitation will allow an attacker to gain access to confidential attribute values. **Solution** Upgrade to Samba 4.8.4 or 4.7.9 or 4.6.16 or later. Please see the references for more information. **Solution type:** VendorFix **Affected Software/OS:** All versions of Samba from 4.0.0 onwards **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exists due to a missing access control checks.							
	Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** Samba 'AD LDAP' Information Disclosure Vulnerability - Aug18 (NVT: 1.3.6.1.4.1.25623.1.0.813784) **Version used:** 2019-07-05T09:54:18+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:S/C:P/I:N/A:N) **CVE:** CVE-2018-10919 **BID:** NOBID **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2018-10919.html, URL:https://www.samba.org/samba/history/samba-4.8.4.html, URL:https://www.samba.org/samba/history/samba-4.7.9.html, URL:https://www.samba.org/samba/history/samba-4.6.16.html						
38.123.140.31 demoweb.clone-systems.com	110/tcp	The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size 2048).	medium	NOCVE	4.0	☐	☒
	Vulnerability Detection Result: Server Temporary Key Size: 1024 bits **Impact:** An attacker might be able to decrypt the SSL/TLS communication offline. **Solution** Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html) **Solution type:** Workaround **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.							
	Vulnerability Detection Method: Checks the DHE temporary public key size. **Details:** SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.106223) **Version used:** $Revision: 4739 $ **References:** **CVSS v2 Vector:** (AV:N/AC:H/Au:N/C:P/I:P/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://weakdh.org/, URL:https://weakdh.org/sysadmin.html						
38.123.140.31 demoweb.clone-systems.com	995/tcp	The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size 2048).	medium	NOCVE	4.0	☐	☒
	Vulnerability Detection Result: Server Temporary Key Size: 1024 bits **Impact:** An attacker might be able to decrypt the SSL/TLS communication offline. **Solution** Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html) **Solution type:** Workaround **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.							
	Vulnerability Detection Method: Checks the DHE temporary public key size. **Details:** SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.106223) **Version used:** $Revision: 4739 $ **References:** **CVSS v2 Vector:** (AV:N/AC:H/Au:N/C:P/I:P/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://weakdh.org/, URL:https://weakdh.org/sysadmin.html						

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	Samba is prone to a privilege escalation vulnerability.	medium	CVE-2016-2126	4.0	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.3.13 Installation path / port: 445/tcp **Impact:** Successful exploitation would allow an authenticated attacker to gain additional access rights. **Solution** Update to version 4.3.13, 4.4.8 or 4.5.3 respectively. **Solution type:** VendorFix **Affected Software/OS:** Samba versions 4.0.0 through 4.3.12, 4.4.0 through 4.4.7 and 4.5.0 through 4.5.2. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Samba is prone to privilege elevation due to incorrect handling of the PAC (Privilege Attribute Certificate) checksum. A remote, authenticated, attacker can cause the winbindd process to creash using a legitimate Kerberos ticket. A local service with access to the winbindd privileged pipe can cause winbindd to cache elevated access permissions.						
						Vulnerability Detection Method: Checks if a vulnerable version is present on the target host. **Details:** Samba >= 4.0.0, = 4.5.2 Privilege Escalation Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.113287) **Version used:** $Revision: 12236 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:S/C:N/I:N/A:P) **CVE:** CVE-2016-2126 **BID:** 94994 **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2016-2126.html	
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to overwrite ACLs vulnerability.	medium	CVE-2015-7560	4.0	☐	☒
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.1.23 Installation path / port: 445/tcp **Impact:** Successful exploitation will allow a remote attacker to gain access to an arbitrary file or directory by overwriting its ACL. Impact Level: Application **Solution** Upgrade to Samba version 4.1.23 or 4.2.9 or 4.3.6 or 4.4.0rc4 or later. For updates refer to https://www.samba.org **Solution type:** VendorFix **Affected Software/OS:** Samba versions 3.2.x and 4.x before 4.1.23, 4.2.x before 4.2.9, 4.3.x before 4.3.6 and 4.4.x before 4.4.0rc4. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** The flaw exist due to an improper handling of the request,a UNIX SMB1 call, to create a symlink.						
						Vulnerability Detection Method: Get the installed version with the help of detect NVT and check the version is vulnerable or not. **Details:** Samba Overwrite ACLs Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.807711) **Version used:** $Revision: 4401 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:S/C:N/I:P/A:N) **CVE:** CVE-2015-7560 **BID:** NOBID **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2015-7560.html	
38.123.140.31 demoweb.clone-systems.com	25/tcp	The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size 2048).	medium	NOCVE	4.0	☐	☒
	Vulnerability Detection Result: Server Temporary Key Size: 1024 bits **Impact:** An attacker might be able to decrypt the SSL/TLS communication offline. **Solution** Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html) **Solution type:** Workaround **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.						
						Vulnerability Detection Method: Checks the DHE temporary public key size. **Details:** SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability (NVT: 1.3.6.1.4.1.25623.1.0.106223) **Version used:** $Revision: 4739 $ **References:** **CVSS v2 Vector:** (AV:N/AC:H/Au:N/C:P/I:P/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://weakdh.org/, URL:https://weakdh.org/sysadmin.html	

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	Samba is prone to a privilege delegation vulnerability.	low	CVE-2016-2125	3.3	☒	☐
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.3.13 Installation path / port: 445/tcp **Impact:** Successful exploitation would allow an authenticated attacker to gain additional access rights. **Solution** Update to version 4.3.13, 4.4.8 or 4.5.3 respectively. **Solution type:** VendorFix **Affected Software/OS:** Samba versions 3.0.25 through 4.3.12, 4.4.0 through 4.4.7 and 4.5.0 through 4.5.2. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Samba always requests forwardable tickets when using Kerberos authentication. A service to which Samba authenticated using Kerberos could subsequently use the ticket to impersonate Samba to other services or domain users.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba >= 3.0.25, = 4.5.2 Multiple Vulnerabilities (NVT: 1.3.6.1.4.1.25623.1.0.113288) **Version used:** $Revision: 13394 $ **References:** **CVSS v2 Vector:** (AV:A/AC:L/Au:N/C:P/I:N/A:N) **CVE:** CVE-2016-2125 **BID:** NOBID **CERT:** **XREF:** URL:https://www.samba.org/samba/security/CVE-2016-2125.html		
38.123.140.31 demoweb.clone-systems.com	445/tcp	This host is running Samba and is prone to multiple denial-of-service vulnerabilities.	low	CVE-2014-0244, CVE-2014-3493	3.3	☒	☐
	Vulnerability Detection Result: Installed version: 4.1.6 Fixed version: 4.1.9 Installation path / port: 445/tcp **Impact:** Successfully exploiting this issue will allow remote attackers to cause a denial-of-service condition. **Solution** Upgrade to Samba 3.6.24 or 4.0.19 or 4.1.9 or later. **Solution type:** VendorFix **Affected Software/OS:** Samba Server versions 3.6.x before 3.6.24, 4.0.x before 4.0.19, and 4.1.x before 4.1.9. **Detection Reliability:** Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches. **Vulnerability Insight:** Multiple flaws exists due to, - An error in the nmbd NetBIOS name services daemon which causes the nmbd server to loop the CPU. - A memory corruption error. A valid unicode path names stored on disk can cause smbd to crash if an authenticated client attempts to read them using a non-unicode request.				**Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **Details:** Samba 'smbd and nmbd' Multiple Denial-of-Service Vulnerabilities (NVT: 1.3.6.1.4.1.25623.1.0.811219) **Version used:** $Revision: 14173 $ **References:** **CVSS v2 Vector:** (AV:A/AC:L/Au:N/C:N/I:N/A:P) **CVE:** CVE-2014-0244, CVE-2014-3493 **BID:** 68148, 68150 **CERT:** **XREF:** URL:http://www.securitytracker.com/id/1030455, URL:http://www.samba.org/samba/security/CVE-2014-3493, URL:http://www.samba.org/samba/security/CVE-2014-0244		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	general/tcp	The remote host implements TCP timestamps and therefore allows to compute the uptime.	low	NOCVE	2.6	☒	☐
	Vulnerability Detection Result: It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 670168084 Packet 2: 670168356 **Impact:** A side effect of this feature is that the uptime of the remote host can sometimes be computed. **Solution** To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152 **Solution type:** Mitigation **Affected Software/OS:** TCP/IPv4 implementations that implement RFC1323. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The remote host implements TCP timestamps, as defined by RFC1323.						
38.123.140.31 demoweb.clone-systems.com	22/tcp	The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.	low	NOCVE	2.6	☒	☐
	Vulnerability Detection Result: The following weak client-to-server MAC algorithms are supported by the remote service: hmac-md5 hmac-md5-96 hmac-md5-96-etm@openssh.com hmac-md5-etm@openssh.com hmac-sha1-96 hmac-sha1-96-etm@openssh.com The following weak server-to-client MAC algorithms are supported by the remote service: hmac-md5 hmac-md5-96 hmac-md5-96-etm@openssh.com hmac-md5-etm@openssh.com hmac-sha1-96 hmac-sha1-96-etm@openssh.com **Solution** Disable the weak MAC algorithms. **Solution type:** Mitigation **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response shows the likely presence of the vulnerable application or of the vulnerability. "Likely" means that only rare circumstances are possible where the detection would be wrong.						

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	143/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *6 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** $Revision: 4743 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			
38.123.140.31 demoweb.clone-systems.com	993/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *7 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** $Revision: 4743 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			
38.123.140.31 demoweb.clone-systems.com	995/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *8 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** $Revision: 4743 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			
38.123.140.31 demoweb.clone-systems.com	110/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *9 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** $Revision: 4743 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	8082/tcp	The script consolidates various information for CGI scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community portal.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The Hostname/IP "demoweb.clone-systems.com" was used to access the remote host. Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use. Requests to this service are done via HTTP/1.1. This service seems to be able to host PHP scripts. This service seems to be NOT able to host ASP scripts. The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host. Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use. The following directories were used for CGI scanning: http://demoweb.clone-systems.com:8082/ While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)" http://demoweb.clone-systems.com:8082/icons **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** CGI Scanning Consolidation (NVT: 1.3.6.1.4.1.25623.1.0.111038) **Version used:** 2019-09-23T09:25:24+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://community.greenbone.net/c/vulnerability-tests			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	80/tcp	The script consolidates various information for CGI scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community portal.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The Hostname/IP "demoweb.clone-systems.com" was used to access the remote host. Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use. Requests to this service are done via HTTP/1.1. This service seems to be able to host PHP scripts. This service seems to be NOT able to host ASP scripts. The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host. Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use. The following directories were used for CGI scanning: http://demoweb.clone-systems.com/ While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)" http://demoweb.clone-systems.com/icons **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** CGI Scanning Consolidation (NVT: 1.3.6.1.4.1.25623.1.0.111038) **Version used:** 2019-09-23T09:25:24+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://community.greenbone.net/c/vulnerability-tests			
38.123.140.31 demoweb.clone-systems.com	general/tcp	This script consolidates the OS information detected by several NVTs and tries to find the best matching OS. Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection. If any of this information is wrong or could be improved please consider to report these to the referenced community portal.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *10 (Click here to access the vulnerability details) **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** OS Detection Consolidation and Reporting (NVT: 1.3.6.1.4.1.25623.1.0.105937) **Version used:** 2019-10-29T11:11:51+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://community.greenbone.net/c/vulnerability-tests			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	80/tcp	Detects the installed version of Apache Web Server The script detects the version of Apache HTTP Server on remote host and sets the KB.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Detected Apache Version: 2.4.7 Location: 80/tcp CPE: cpe:/a:apache:http_server:2.4.7 Concluded from version/product identification result: Server: Apache/2.4.7 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Apache Web Server Detection (NVT: 1.3.6.1.4.1.25623.1.0.900498) **Version used:** 2019-10-16T09:54:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	993/tcp	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	low	CVE-2016-0800, CVE-2014-3566	0.0	☒	☐
	Vulnerability Detection Result: TLS version 1.1 was detected. It shares some cryptography libraries with TLSv1.0 and it is not reccomended to be used in your environment. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 and TLSv1.0 and/or TLSv1.1 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The TLSv1.0 and TLSv1.1 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.300008) **Version used:** $Revision: 1020 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2016-0800, CVE-2014-3566 **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/, URL:https://drownattack.com/, URL:https://www.imperialviolet.org/2014/10/14/poodle.html			
38.123.140.31 demoweb.clone-systems.com	80/tcp	This detects the HTTP Server's type and version.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The remote web server type is : Apache/2.4.7 (Ubuntu) Solution : You can set the directive "ServerTokens Prod" to limit the information emanating from the server in its response headers. **Solution** Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** HTTP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10107) **Version used:** $Revision: 3564 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	8082/tcp	This detects the HTTP Server's type and version.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The remote web server type is : Apache/2.4.7 (Ubuntu) Solution : You can set the directive "ServerTokens Prod" to limit the information emanating from the server in its response headers. **Solution** Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** HTTP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10107) **Version used:** $Revision: 3564 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	995/tcp	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	low	CVE-2016-0800, CVE-2014-3566	0.0	☒	☐
	Vulnerability Detection Result: TLS version 1.1 was detected. It shares some cryptography libraries with TLSv1.0 and it is not reccomended to be used in your environment. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 and TLSv1.0 and/or TLSv1.1 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The TLSv1.0 and TLSv1.1 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.300008) **Version used:** $Revision: 1020 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2016-0800, CVE-2014-3566 **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/, URL:https://drownattack.com/, URL:https://www.imperialviolet.org/2014/10/14/poodle.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	995/tcp	The SSL/TLS certificate contains a common name (CN) that does not match the hostname.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The certificate of the remote service contains a common name (CN) that does not match the hostname "demoweb.clone-systems.com". Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server serial ....: 00CC6C568D704F8BBE valid from : 2016-08-09 13:18:58 UTC valid until: 2026-08-09 13:18:58 UTC fingerprint (SHA-1): 84C192E09BD30A3A0707042BB2181A731AFF09BE fingerprint (SHA-256): 45B822C7CCD2315D9B09BDF9F6E296315052A42057EFE51872FA7E6BDDEE1FBA **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN (NVT: 1.3.6.1.4.1.25623.1.0.103141) **Version used:** $Revision: 4836 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			
38.123.140.31 demoweb.clone-systems.com	general/tcp	This plugin checks to find live hosts and all their associated open ports. Several methods are used for this depending on configuration of this check.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The following ports were discovered with open state allowing TCP connections: 22/tcp open ssh 25/tcp open smtp 53/tcp open domain 80/tcp open http 110/tcp open pop3 139/tcp open netbios-ssn 143/tcp open imap 445/tcp open microsoft-ds 993/tcp open imaps 995/tcp open pop3s 3306/tcp open mysql 8082/tcp open blackice-alerts **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Host Detection (NVT: 1.3.6.1.4.1.25623.1.0.14259) **Version used:** 2019-09-09T06:03:58+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://nmap.org/, URL:https://nmap.org/book/performance-timing-templates.html, URL:https://nmap.org/book/man-performance.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	143/tcp	The SSL/TLS certificate contains a common name (CN) that does not match the hostname.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The certificate of the remote service contains a common name (CN) that does not match the hostname "demoweb.clone-systems.com". Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server serial ....: 00CC6C568D704F8BBE valid from : 2016-08-09 13:18:58 UTC valid until: 2026-08-09 13:18:58 UTC fingerprint (SHA-1): 84C192E09BD30A3A0707042BB2181A731AFF09BE fingerprint (SHA-256): 45B822C7CCD2315D9B09BDF9F6E296315052A42057EFE51872FA7E6BDDEE1FBA **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN (NVT: 1.3.6.1.4.1.25623.1.0.103141) **Version used:** $Revision: 4836 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			
38.123.140.31 demoweb.clone-systems.com	25/tcp	The SSL/TLS certificate contains a common name (CN) that does not match the hostname.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The certificate of the remote service contains a common name (CN) that does not match the hostname "demoweb.clone-systems.com". Certificate details: subject ...: CN=demmoweb.clone-systems.com subject alternative names (SAN): None issued by .: CN=demmoweb.clone-systems.com serial ....: 00B17B21E9A6FBE245 valid from : 2016-08-09 13:18:51 UTC valid until: 2026-08-07 13:18:51 UTC fingerprint (SHA-1): DB44833A630E7E4F23034D53D68F3BAD0EB77AC7 fingerprint (SHA-256): 4A4E363A297800EBEFCC1FDCCF2BF82D53BFF390499341A6ADCB57AF9473DD5D **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN (NVT: 1.3.6.1.4.1.25623.1.0.103141) **Version used:** $Revision: 4836 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	110/tcp	The SSL/TLS certificate contains a common name (CN) that does not match the hostname.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The certificate of the remote service contains a common name (CN) that does not match the hostname "demoweb.clone-systems.com". Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server serial ....: 00CC6C568D704F8BBE valid from : 2016-08-09 13:18:58 UTC valid until: 2026-08-09 13:18:58 UTC fingerprint (SHA-1): 84C192E09BD30A3A0707042BB2181A731AFF09BE fingerprint (SHA-256): 45B822C7CCD2315D9B09BDF9F6E296315052A42057EFE51872FA7E6BDDEE1FBA **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN (NVT: 1.3.6.1.4.1.25623.1.0.103141) **Version used:** $Revision: 4836 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			
38.123.140.31 demoweb.clone-systems.com	993/tcp	The SSL/TLS certificate contains a common name (CN) that does not match the hostname.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The certificate of the remote service contains a common name (CN) that does not match the hostname "demoweb.clone-systems.com". Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server serial ....: 00CC6C568D704F8BBE valid from : 2016-08-09 13:18:58 UTC valid until: 2026-08-09 13:18:58 UTC fingerprint (SHA-1): 84C192E09BD30A3A0707042BB2181A731AFF09BE fingerprint (SHA-256): 45B822C7CCD2315D9B09BDF9F6E296315052A42057EFE51872FA7E6BDDEE1FBA **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN (NVT: 1.3.6.1.4.1.25623.1.0.103141) **Version used:** $Revision: 4836 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	It was possible to login using the provided SMB credentials. Hence authenticated checks are enabled.	low	NOCVE	0.0	☒	☐
	Detection Reliability: Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SMB Login Successful For Authenticated Checks (NVT: 1.3.6.1.4.1.25623.1.0.108539) **Version used:** $Revision: 13248 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	25/tcp	The SSL/TLS certificate on this port is self-signed.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The certificate of the remote service is self signed. Certificate details: subject ...: CN=demmoweb.clone-systems.com subject alternative names (SAN): None issued by .: CN=demmoweb.clone-systems.com serial ....: 00B17B21E9A6FBE245 valid from : 2016-08-09 13:18:51 UTC valid until: 2026-08-07 13:18:51 UTC fingerprint (SHA-1): DB44833A630E7E4F23034D53D68F3BAD0EB77AC7 fingerprint (SHA-256): 4A4E363A297800EBEFCC1FDCCF2BF82D53BFF390499341A6ADCB57AF9473DD5D **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Certificate - Self-Signed Certificate Detection (NVT: 1.3.6.1.4.1.25623.1.0.103140) **Version used:** $Revision: 4765 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:http://en.wikipedia.org/wiki/Self-signed_certificate				
38.123.140.31 demoweb.clone-systems.com	143/tcp	The SSL/TLS certificate on this port is self-signed.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The certificate of the remote service is self signed. Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server serial ....: 00CC6C568D704F8BBE valid from : 2016-08-09 13:18:58 UTC valid until: 2026-08-09 13:18:58 UTC fingerprint (SHA-1): 84C192E09BD30A3A0707042BB2181A731AFF09BE fingerprint (SHA-256): 45B822C7CCD2315D9B09BDF9F6E296315052A42057EFE51872FA7E6BDDEE1FBA **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Certificate - Self-Signed Certificate Detection (NVT: 1.3.6.1.4.1.25623.1.0.103140) **Version used:** $Revision: 4765 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:http://en.wikipedia.org/wiki/Self-signed_certificate				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	The host has enabled SMBv1 for the SMB Server.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: SMBv1 is enabled for the SMB Server **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Vulnerability Detection Method:** Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT: - SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830). **Details:** SMBv1 enabled (Remote Check) (NVT: 1.3.6.1.4.1.25623.1.0.140151) **Version used:** 2019-05-20T06:24:13+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices, URL:https://support.microsoft.com/en-us/kb/2696547, URL:https://support.microsoft.com/en-us/kb/204279			
38.123.140.31 demoweb.clone-systems.com	general/CPE-T	This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan. Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: 38.123.140.31|cpe:/a:apache:http_server:2.4.7 38.123.140.31|cpe:/a:dovecot:dovecot 38.123.140.31|cpe:/a:isc:bind:9.9.5.3 38.123.140.31|cpe:/a:openbsd:openssh:6.6.1p1 38.123.140.31|cpe:/a:oracle:mysql 38.123.140.31|cpe:/a:postfix:postfix 38.123.140.31|cpe:/a:samba:samba:4.1.6 38.123.140.31|cpe:/o:canonical:ubuntu_linux:14.04 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** CPE Inventory (NVT: 1.3.6.1.4.1.25623.1.0.810002) **Version used:** 2019-10-24T11:29:24+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://nvd.nist.gov/products/cpe			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	995/tcp	The SSL/TLS certificate on this port is self-signed.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The certificate of the remote service is self signed. Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server serial ....: 00CC6C568D704F8BBE valid from : 2016-08-09 13:18:58 UTC valid until: 2026-08-09 13:18:58 UTC fingerprint (SHA-1): 84C192E09BD30A3A0707042BB2181A731AFF09BE fingerprint (SHA-256): 45B822C7CCD2315D9B09BDF9F6E296315052A42057EFE51872FA7E6BDDEE1FBA **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Certificate - Self-Signed Certificate Detection (NVT: 1.3.6.1.4.1.25623.1.0.103140) **Version used:** $Revision: 4765 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:http://en.wikipedia.org/wiki/Self-signed_certificate			
38.123.140.31 demoweb.clone-systems.com	445/tcp	The script detects the Windows SMB Accessible Shares and sets the result into KB.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The following shares were found IPC$ **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Microsoft Windows SMB Accessible Shares (NVT: 1.3.6.1.4.1.25623.1.0.902425) **Version used:** $Revision: 3690 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	110/tcp	The SSL/TLS certificate on this port is self-signed.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The certificate of the remote service is self signed. Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server serial ....: 00CC6C568D704F8BBE valid from : 2016-08-09 13:18:58 UTC valid until: 2026-08-09 13:18:58 UTC fingerprint (SHA-1): 84C192E09BD30A3A0707042BB2181A731AFF09BE fingerprint (SHA-256): 45B822C7CCD2315D9B09BDF9F6E296315052A42057EFE51872FA7E6BDDEE1FBA **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.					
38.123.140.31 demoweb.clone-systems.com	995/tcp	This detects the POP3 Server's type and version by connecting to the server and processing the received banner.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Remote POP3 server banner: +OK Dovecot (Ubuntu) ready. This is probably: - Dovecot The remote POP3 server is announcing the following available CAPABILITIES via an encrypted connection: AUTH-RESP-CODE, CAPA, PIPELINING, RESP-CODES, SASL PLAIN, TOP, UIDL, USER **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.					
38.123.140.31 demoweb.clone-systems.com	110/tcp	This detects the POP3 Server's type and version by connecting to the server and processing the received banner.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Remote POP3 server banner: +OK Dovecot (Ubuntu) ready. This is probably: - Dovecot The remote POP3 server is announcing the following available CAPABILITIES via an unencrypted connection: AUTH-RESP-CODE, CAPA, PIPELINING, RESP-CODES, SASL, STLS, TOP, UIDL **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.					

	Details: SSL/TLS: Certificate - Self-Signed Certificate Detection (NVT: 1.3.6.1.4.1.25623.1.0.103140) **Version used:** $Revision: 4765 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:http://en.wikipedia.org/wiki/Self-signed_certificate
	Details: POP3 Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10185) **Version used:** 2019-10-09T06:13:56+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF
	Details: POP3 Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10185) **Version used:** 2019-10-09T06:13:56+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	general/icmp	The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.	low	CVE-1999-0524	0.0	☒	☐
	Detection Reliability: Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** ICMP Timestamp Detection (NVT: 1.3.6.1.4.1.25623.1.0.103190) **Version used:** $Revision: 3115 $ **References:** **CVSS v2 Vector:** (AV:L/AC:L/Au:N/C:N/I:N/A:N) **CVE:** CVE-1999-0524 **BID:** NOBID **CERT:** **XREF:** URL:http://www.ietf.org/rfc/rfc0792.txt				
38.123.140.31 demoweb.clone-systems.com	25/tcp	The script checks the SMTP server banner for the presence of Postfix.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Detected Postfix Version: unknown Location: 25/tcp CPE: cpe:/a:postfix:postfix Concluded from version/product identification result: 220 demmoweb.clone-systems.com ESMTP Postfix (Ubuntu) **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Postfix SMTP Server Detection (NVT: 1.3.6.1.4.1.25623.1.0.111086) **Version used:** $Revision: 2598 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	993/tcp	The SSL/TLS certificate on this port is self-signed.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The certificate of the remote service is self signed. Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F744064656D6D6F7765622E636C6F6E652D73797374656D732E636F6D,CN=localhost,OU=localhost,O=Dovecot mail server serial ....: 00CC6C568D704F8BBE valid from : 2016-08-09 13:18:58 UTC valid until: 2026-08-09 13:18:58 UTC fingerprint (SHA-1): 84C192E09BD30A3A0707042BB2181A731AFF09BE fingerprint (SHA-256): 45B822C7CCD2315D9B09BDF9F6E296315052A42057EFE51872FA7E6BDDEE1FBA **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Certificate - Self-Signed Certificate Detection (NVT: 1.3.6.1.4.1.25623.1.0.103140) **Version used:** $Revision: 4765 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:http://en.wikipedia.org/wiki/Self-signed_certificate				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	8082/tcp	Detects the installed version of Apache Web Server The script detects the version of Apache HTTP Server on remote host and sets the KB.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Detected Apache Version: 2.4.7 Location: 8082/tcp CPE: cpe:/a:apache:http_server:2.4.7 Concluded from version/product identification result: Server: Apache/2.4.7 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Apache Web Server Detection (NVT: 1.3.6.1.4.1.25623.1.0.900498) **Version used:** 2019-10-16T09:54:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	25/tcp	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	low	CVE-2016-0800, CVE-2014-3566	0.0	☒	☐
	Vulnerability Detection Result: TLS version 1.1 was detected. It shares some cryptography libraries with TLSv1.0 and it is not reccomended to be used in your environment. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 and TLSv1.0 and/or TLSv1.1 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The TLSv1.0 and TLSv1.1 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.300008) **Version used:** $Revision: 1020 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2016-0800, CVE-2014-3566 **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/, URL:https://drownattack.com/, URL:https://www.imperialviolet.org/2014/10/14/poodle.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	110/tcp	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	low	CVE-2016-0800, CVE-2014-3566	0.0	☒	☐
	Vulnerability Detection Result: TLS version 1.1 was detected. It shares some cryptography libraries with TLSv1.0 and it is not reccomended to be used in your environment. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 and TLSv1.0 and/or TLSv1.1 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The TLSv1.0 and TLSv1.1 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.300008) **Version used:** $Revision: 1020 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2016-0800, CVE-2014-3566 **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/, URL:https://drownattack.com/, URL:https://www.imperialviolet.org/2014/10/14/poodle.html			
38.123.140.31 demoweb.clone-systems.com	143/tcp	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	low	CVE-2016-0800, CVE-2014-3566	0.0	☒	☐
	Vulnerability Detection Result: TLS version 1.1 was detected. It shares some cryptography libraries with TLSv1.0 and it is not reccomended to be used in your environment. **Impact:** An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. **Solution** It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols. Please see the references for more information. **Solution type:** Mitigation **Affected Software/OS:** All services providing an encrypted communication using the SSLv2 and/or SSLv3 and TLSv1.0 and/or TLSv1.1 protocols. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** The TLSv1.0 and TLSv1.1 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)		**Vulnerability Detection Method:** Check the used protocols of the services provided by this system. **Details:** TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (NVT: 1.3.6.1.4.1.25623.1.0.300008) **Version used:** $Revision: 1020 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2016-0800, CVE-2014-3566 **BID:** NOBID **CERT:** **XREF:** URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/, URL:https://drownattack.com/, URL:https://www.imperialviolet.org/2014/10/14/poodle.html			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	The host has enabled SMBv1 for the SMB Server.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: SMBv1 is enabled for the SMB Server **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Vulnerability Detection Method:** Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT: - SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830). **Details:** SMBv1 enabled (Remote Check) (NVT: 1.3.6.1.4.1.25623.1.0.140151) **Version used:** 2019-05-20T06:24:13+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices, URL:https://support.microsoft.com/en-us/kb/2696547, URL:https://support.microsoft.com/en-us/kb/204279			
38.123.140.31 demoweb.clone-systems.com	25/tcp	This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.	low	CVE-2013-2566, CVE-2015-4000	0.0	☒	☐
	Vulnerability Detection Result: *11 (Click here to access the vulnerability details) **Solution** The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task. **Solution type:** Mitigation **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566). - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000). - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong		**Details:** SSL/TLS: Report Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103440) **Version used:** $Revision: 4863 $ **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** CVE-2013-2566, CVE-2015-4000 **BID:** NOBID **CERT:** **XREF:** URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html, URL:https://bettercrypto.org/, URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/			
38.123.140.31 demoweb.clone-systems.com	445/tcp	Detection of Server Message Block(SMB). This script sends SMB Negotiation request and try to get the version from the response.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: SMBv1, SMBv2 and SMBv3 are enabled on remote target **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SMB Remote Version Detection (NVT: 1.3.6.1.4.1.25623.1.0.807830) **Version used:** $Revision: 4262 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	general/tcp	It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The following additional but not resolvable hostnames were detected: demmoweb.clone-systems.com **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Hostname discovery from server certificate (NVT: 1.3.6.1.4.1.25623.1.0.111010) **Version used:** $Revision: 13774 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			
38.123.140.31 demoweb.clone-systems.com	143/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=demmoweb.clone-systems.com subject alternative names (SAN): None issued by .: CN=demmoweb.clone-systems.com serial ....: 00B17B21E9A6FBE245 valid from : 2016-08-09 13:18:51 UTC valid until: 2026-08-07 13:18:51 UTC fingerprint (SHA-1): DB44833A630E7E4F23034D53D68F3BAD0EB77AC7 fingerprint (SHA-256): 4A4E363A297800EBEFCC1FDCCF2BF82D53BFF390499341A6ADCB57AF9473DD5D **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** $Revision: 4768 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			
38.123.140.31 demoweb.clone-systems.com	25/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *12 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** $Revision: 4771 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	110/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *13 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** $Revision: 4771 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	25/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=demmoweb.clone-systems.com subject alternative names (SAN): None issued by .: CN=demmoweb.clone-systems.com serial ....: 00B17B21E9A6FBE245 valid from : 2016-08-09 13:18:51 UTC valid until: 2026-08-07 13:18:51 UTC fingerprint (SHA-1): DB44833A630E7E4F23034D53D68F3BAD0EB77AC7 fingerprint (SHA-256): 4A4E363A297800EBEFCC1FDCCF2BF82D53BFF390499341A6ADCB57AF9473DD5D **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** $Revision: 4768 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	995/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=demmoweb.clone-systems.com subject alternative names (SAN): None issued by .: CN=demmoweb.clone-systems.com serial ....: 00B17B21E9A6FBE245 valid from : 2016-08-09 13:18:51 UTC valid until: 2026-08-07 13:18:51 UTC fingerprint (SHA-1): DB44833A630E7E4F23034D53D68F3BAD0EB77AC7 fingerprint (SHA-256): 4A4E363A297800EBEFCC1FDCCF2BF82D53BFF390499341A6ADCB57AF9473DD5D **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** $Revision: 4768 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	995/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *14 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** $Revision: 4736 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	22/tcp	This script detects which algorithms are supported by the remote SSH Service.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *15 (Click here to access the vulnerability details) **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SSH Protocol Algorithms Supported (NVT: 1.3.6.1.4.1.25623.1.0.105565) **Version used:** 2019-10-28T15:06:41+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	995/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *16 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** $Revision: 4771 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	110/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *17 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** $Revision: 4736 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	25/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *18 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** $Revision: 4736 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	110/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=demmoweb.clone-systems.com subject alternative names (SAN): None issued by .: CN=demmoweb.clone-systems.com serial ....: 00B17B21E9A6FBE245 valid from : 2016-08-09 13:18:51 UTC valid until: 2026-08-07 13:18:51 UTC fingerprint (SHA-1): DB44833A630E7E4F23034D53D68F3BAD0EB77AC7 fingerprint (SHA-256): 4A4E363A297800EBEFCC1FDCCF2BF82D53BFF390499341A6ADCB57AF9473DD5D **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** $Revision: 4768 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	143/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *19 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** $Revision: 4771 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	993/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *20 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** $Revision: 4736 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	143/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *21 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** $Revision: 4736 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	80/tcp	All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Missing Headers --- Content-Security-Policy Referrer-Policy X-Content-Type-Options X-Frame-Options X-Permitted-Cross-Domain-Policies X-XSS-Protection **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** HTTP Security Headers Detection (NVT: 1.3.6.1.4.1.25623.1.0.112081) **Version used:** $Revision: 10899 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project, URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers, URL:https://securityheaders.io/			
38.123.140.31 demoweb.clone-systems.com	8082/tcp	All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Missing Headers --- Content-Security-Policy Referrer-Policy X-Content-Type-Options X-Frame-Options X-Permitted-Cross-Domain-Policies X-XSS-Protection **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** HTTP Security Headers Detection (NVT: 1.3.6.1.4.1.25623.1.0.112081) **Version used:** $Revision: 10899 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project, URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers, URL:https://securityheaders.io/			
38.123.140.31 demoweb.clone-systems.com	22/tcp	Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service. The following versions are tried: 1.33, 1.5, 1.99 and 2.0	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The remote SSH Server supports the following SSH Protocol Versions: 1.99 2.0 SSHv2 Fingerprint(s): ecdsa-sha2-nistp256: b7:70:6a:be:91:0f:4e:37:fb:0b:b5:91:95:b4:b2:b7 ssh-dss: d7:2e:3b:38:5b:5d:ec:d8:89:6c:d4:81:1b:df:d5:6d ssh-rsa: e6:99:73:66:5c:7e:13:59:d3:ab:9e:5d:61:9a:b0:84 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response shows the likely presence of the vulnerable application or of the vulnerability. "Likely" means that only rare circumstances are possible where the detection would be wrong.		**Details:** SSH Protocol Versions Supported (NVT: 1.3.6.1.4.1.25623.1.0.100259) **Version used:** $Revision: 4484 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	general/tcp	Reports Dovecot installation including version and location.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *22 (Click here to access the vulnerability details) **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Dovecot Detection (Consolidation) (NVT: 1.3.6.1.4.1.25623.1.0.113212) **Version used:** $Revision: 13403 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.dovecot.org/				
38.123.140.31 demoweb.clone-systems.com	993/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *23 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** $Revision: 4771 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	993/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=demmoweb.clone-systems.com subject alternative names (SAN): None issued by .: CN=demmoweb.clone-systems.com serial ....: 00B17B21E9A6FBE245 valid from : 2016-08-09 13:18:51 UTC valid until: 2026-08-07 13:18:51 UTC fingerprint (SHA-1): DB44833A630E7E4F23034D53D68F3BAD0EB77AC7 fingerprint (SHA-256): 4A4E363A297800EBEFCC1FDCCF2BF82D53BFF390499341A6ADCB57AF9473DD5D **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** $Revision: 4768 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	general/tcp	The script reports a detected OpenSSH including the version number.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Detected OpenSSH Server Version: 6.6.1p1 Location: 22/tcp CPE: cpe:/a:openbsd:openssh:6.6.1p1 Concluded from version/product identification result: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** OpenSSH Detection Consolidation (NVT: 1.3.6.1.4.1.25623.1.0.108577) **Version used:** 2019-05-23T06:42:35+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.openssh.com/				
38.123.140.31 demoweb.clone-systems.com	53/tcp	BIND 'NAMED' is an open-source DNS server from ISC.org. Many proprietary DNS servers are based on BIND source code.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Detected Bind Version: 9.9.5.3 Location: 53/tcp CPE: cpe:/a:isc:bind:9.9.5.3 Concluded from version/product identification result: 9.9.5-3-Ubuntu **Solution** Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The BIND based NAMED servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source.		**Details:** Determine which version of BIND name daemon is running (NVT: 1.3.6.1.4.1.25623.1.0.10028) **Version used:** $Revision: 4542 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	53/tcp	A DNS Server is running at this Host. A Name Server translates domain names into IP addresses. This makes it possible for a user to access a website by typing in the domain name instead of the website's actual IP address.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The remote DNS server banner is: 9.9.5-3-Ubuntu **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** DNS Server Detection (TCP) (NVT: 1.3.6.1.4.1.25623.1.0.108018) **Version used:** $Revision: 4463 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	general/tcp	A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Here is the route from 38.123.140.119 to 38.123.140.31: 38.123.140.119 38.123.140.31 **Solution** Block unwanted packets from escaping your network. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Traceroute (NVT: 1.3.6.1.4.1.25623.1.0.51662) **Version used:** 2019-09-09T06:03:58+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	445/tcp	It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Detected Samba Version: 4.1.6 Location: 445/tcp CPE: cpe:/a:samba:samba:4.1.6 Concluded from version/product identification result: Samba 4.1.6-Ubuntu Extra information: Detected SMB workgroup: WORKGROUP Detected SMB server: Samba 4.1.6-Ubuntu **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response shows the likely presence of the vulnerable application or of the vulnerability. "Likely" means that only rare circumstances are possible where the detection would be wrong.		**Details:** SMB NativeLanMan (NVT: 1.3.6.1.4.1.25623.1.0.102011) **Version used:** 2019-10-22T06:50:15+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	445/tcp	This script attempts to logon into the remote host using login/password credentials.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: It was possible to log into the remote host using the SMB protocol. **Detection Reliability:** Authenticated registry-based checks for Windows systems.		**Details:** SMB log in (NVT: 1.3.6.1.4.1.25623.1.0.10394) **Version used:** 2019-10-16T06:21:07+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Detected SMB workgroup: WORKGROUP Detected SMB server: Samba 4.1.6-Ubuntu Detected OS: Ubuntu 14.04 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response shows the likely presence of the vulnerable application or of the vulnerability. "Likely" means that only rare circumstances are possible where the detection would be wrong.		**Details:** SMB NativeLanMan (NVT: 1.3.6.1.4.1.25623.1.0.102011) **Version used:** 2019-10-22T06:50:15+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	25/tcp	Check if the remote Mailserver supports the STARTTLS command.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The remote SMTP server supports SSL/TLS with the 'STARTTLS' command. The remote SMTP server is announcing the following available ESMTP commands (EHLO response) before sending the 'STARTTLS' command: 8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, STARTTLS, VRFY The remote SMTP server is announcing the following available ESMTP commands (EHLO response) after sending the 'STARTTLS' command: 8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, VRFY **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SMTP STARTTLS Detection (NVT: 1.3.6.1.4.1.25623.1.0.103118) **Version used:** $Revision: 4683 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	22/tcp	This detects the SSH Server's type and version by connecting to the server and processing the buffer received. This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Remote SSH server banner: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2 Remote SSH supported authentication: password,publickey Remote SSH text/login banner: (not available) This is probably: - OpenSSH Concluded from remote connection attempt with credentials: Login: OpenVAS-VT Password: OpenVAS-VT **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SSH Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10267) **Version used:** 2019-10-30T07:03:08+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	25/tcp	This detects the SMTP Server's type and version by connecting to the server and processing the buffer received.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Remote SMTP server banner: 220 demmoweb.clone-systems.com ESMTP Postfix (Ubuntu) The remote SMTP server is announcing the following available ESMTP commands (EHLO response) via an unencrypted connection: 8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, STARTTLS, VRFY **Solution** Change the login banner to something generic. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SMTP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10263) **Version used:** $Revision: 2599 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	143/tcp	The remote IMAP Server supports the STARTTLS command.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The remote IMAP server supports SSL/TLS with the 'STARTTLS' command. The remote IMAP server is announcing the following CAPABILITIES before sending the 'STARTTLS' command: ENABLE, ID, IDLE, LITERAL+, LOGIN-REFERRALS, LOGINDISABLED, SASL-IR, STARTTLS The remote IMAP server is announcing the following CAPABILITIES after sending the 'STARTTLS' command: AUTH=PLAIN, ENABLE, ID, IDLE, LITERAL+, LOGIN-REFERRALS, SASL-IR **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** IMAP STARTTLS Detection (NVT: 1.3.6.1.4.1.25623.1.0.105007) **Version used:** $Revision: 4683 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	110/tcp	The remote POP3 Server supports the STARTTLS command.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: The remote POP3 server supports SSL/TLS with the 'STLS' command. The remote POP3 server is announcing the following CAPABILITIES before sending the 'STLS' command: AUTH-RESP-CODE, CAPA, PIPELINING, RESP-CODES, SASL, STLS, TOP, UIDL The remote POP3 server is announcing the following CAPABILITIES after sending the 'STLS' command: AUTH-RESP-CODE, CAPA, PIPELINING, RESP-CODES, SASL PLAIN, TOP, UIDL, USER **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** POP3 STARTTLS Detection (NVT: 1.3.6.1.4.1.25623.1.0.105008) **Version used:** $Revision: 4683 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	143/tcp	This detects the IMAP Server's type and version by connecting to the server and processing the received banner.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Remote IMAP server banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED] Dovecot (Ubuntu) ready. * ID ("name" "Dovecot") This is probably: - Dovecot The remote IMAP server is announcing the following available CAPABILITIES via an unencrypted connection: ENABLE, ID, IDLE, LITERAL+, LOGIN-REFERRALS, LOGINDISABLED, SASL-IR, STARTTLS **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** IMAP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.11414) **Version used:** 2019-10-09T06:13:56+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			
38.123.140.31 demoweb.clone-systems.com	3306/tcp	Detects the installed version of MySQL/MariaDB. Detect a running MySQL/MariaDB by getting the banner, extract the version from the banner.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Detected MySQL Version: unknown Location: 3306/tcp CPE: cpe:/a:oracle:mysql Extra information: Scanner received a ER_HOST_NOT_PRIVILEGED error from the remote MySQL server. Some tests may fail. Allow the scanner to access the remote MySQL server for better results. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** MySQL/MariaDB Detection (NVT: 1.3.6.1.4.1.25623.1.0.100152) **Version used:** 2019-11-05T16:13:01+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			
38.123.140.31 demoweb.clone-systems.com	993/tcp	This detects the IMAP Server's type and version by connecting to the server and processing the received banner.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Remote IMAP server banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot (Ubuntu) ready. * ID ("name" "Dovecot") This is probably: - Dovecot The remote IMAP server is announcing the following available CAPABILITIES via an encrypted connection: AUTH=PLAIN, ENABLE, ID, IDLE, LITERAL+, LOGIN-REFERRALS, SASL-IR **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** IMAP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.11414) **Version used:** 2019-10-09T06:13:56+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	110/tcp	This detects the POP3 Server's type and version by connecting to the server and processing the received banner.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Remote POP3 server banner: +OK Dovecot (Ubuntu) ready. This is probably: - Dovecot The remote POP3 server is announcing the following available CAPABILITIES via an unencrypted connection: AUTH-RESP-CODE, CAPA, PIPELINING, RESP-CODES, SASL, STLS, TOP, UIDL **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** POP3 Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10185) **Version used:** 2019-10-09T06:13:56+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	143/tcp	This routine reports all SSL/TLS cipher suites accepted by a service. As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *24 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** $Revision: 4739 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	995/tcp	This detects the POP3 Server's type and version by connecting to the server and processing the received banner.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Remote POP3 server banner: +OK Dovecot (Ubuntu) ready. This is probably: - Dovecot The remote POP3 server is announcing the following available CAPABILITIES via an encrypted connection: AUTH-RESP-CODE, CAPA, PIPELINING, RESP-CODES, SASL PLAIN, TOP, UIDL, USER **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** POP3 Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10185) **Version used:** 2019-10-09T06:13:56+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	110/tcp	This routine reports all SSL/TLS cipher suites accepted by a service. As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *25 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** $Revision: 4739 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	25/tcp	This routine reports all SSL/TLS cipher suites accepted by a service. As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *26 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** $Revision: 4739 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	139/tcp	This script detects wether port 445 and 139 are open and if they are running a CIFS/SMB server.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: A SMB server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SMB/CIFS Server Detection (NVT: 1.3.6.1.4.1.25623.1.0.11011) **Version used:** $Revision: 4261 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	445/tcp	This script detects wether port 445 and 139 are open and if they are running a CIFS/SMB server.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: A CIFS server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SMB/CIFS Server Detection (NVT: 1.3.6.1.4.1.25623.1.0.11011) **Version used:** $Revision: 4261 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	22/tcp	This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: An ssh server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2019-07-08T14:12:44+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	995/tcp	This routine reports all SSL/TLS cipher suites accepted by a service. As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *27 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** $Revision: 4739 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	993/tcp	This routine reports all SSL/TLS cipher suites accepted by a service. As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *28 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** $Revision: 4739 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	80/tcp	This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: A web server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2019-07-08T14:12:44+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	995/tcp	This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: A pop3 server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2019-07-08T14:12:44+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	110/tcp	This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: A pop3 server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2019-07-08T14:12:44+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	general/tcp	This plugin checks to find live hosts and all their associated open ports. Several methods are used for this depending on configuration of this check.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: There are no UDP ports exposed. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Host Detection (NVT: 1.3.6.1.4.1.25623.1.0.14259) **Version used:** 2019-09-09T06:03:58+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://nmap.org/, URL:https://nmap.org/book/performance-timing-templates.html, URL:https://nmap.org/book/man-performance.html				
38.123.140.31 demoweb.clone-systems.com	8082/tcp	This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: A web server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2019-07-08T14:12:44+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	995/tcp	This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: A TLScustom server answered on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2019-07-08T14:12:44+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	993/tcp	This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: A TLScustom server answered on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2019-07-08T14:12:44+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	993/tcp	This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: An IMAP server is running on this port through SSL **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2019-07-08T14:12:44+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	143/tcp	This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: An IMAP server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2019-07-08T14:12:44+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	3306/tcp	This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: A MySQL server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2019-07-08T14:12:44+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				
38.123.140.31 demoweb.clone-systems.com	143/tcp	This detects the IMAP Server's type and version by connecting to the server and processing the received banner.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Remote IMAP server banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED] Dovecot (Ubuntu) ready. * ID ("name" "Dovecot") This is probably: - Dovecot The remote IMAP server is announcing the following available CAPABILITIES via an unencrypted connection: ENABLE, ID, IDLE, LITERAL+, LOGIN-REFERRALS, LOGINDISABLED, SASL-IR, STARTTLS **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** IMAP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.11414) **Version used:** 2019-10-09T06:13:56+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF				

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score	Compliance Status	
						Pass	Fail
38.123.140.31 demoweb.clone-systems.com	993/tcp	This detects the IMAP Server's type and version by connecting to the server and processing the received banner.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: Remote IMAP server banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot (Ubuntu) ready. * ID ("name" "Dovecot") This is probably: - Dovecot The remote IMAP server is announcing the following available CAPABILITIES via an encrypted connection: AUTH=PLAIN, ENABLE, ID, IDLE, LITERAL+, LOGIN-REFERRALS, SASL-IR **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** IMAP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.11414) **Version used:** 2019-10-09T06:13:56+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			
38.123.140.31 demoweb.clone-systems.com	25/tcp	This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: An SMTP server is running on this port Here is its banner : 220 demmoweb.clone-systems.com ESMTP Postfix (Ubuntu) **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2019-07-08T14:12:44+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			
38.123.140.31 demoweb.clone-systems.com	25/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0	☒	☐
	Vulnerability Detection Result: *29 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** $Revision: 4743 $ **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF			

*1 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 25/tcp

'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

*2 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 110/tcp

'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

*3 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 143/tcp

'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

*4 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 993/tcp

'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

*5 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 995/tcp

'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

*6 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 143/tcp

'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

*7 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 993/tcp

'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

*8 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 995/tcp

'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

*9 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 110/tcp

'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

*10 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - general/tcp

Best matching OS:
OS: Ubuntu
Version: 14.04
CPE: cpe:/o:canonical:ubuntu_linux:14.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.108014 (DNS Server OS Identification)
Concluded from DNS server banner on port 53/tcp: 9.9.5-3-Ubuntu
OS: Ubuntu
Version: 14.04
CPE: cpe:/o:canonical:ubuntu_linux:14.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp:
OS String: Unix
SMB String: Samba 4.1.6-Ubuntu
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.4.7 (Ubuntu)
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server default page on port 80/tcp: title>Apache2 Ubuntu Default Page
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 8082/tcp: Server: Apache/2.4.7 (Ubuntu)
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server default page on port 8082/tcp: title>Apache2 Ubuntu Default Page
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111068 (SMTP/POP3/IMAP Server OS Identification)
Concluded from SMTP banner on port 25/tcp: 220 demmoweb.clone-systems.com ESMTP Postfix (Ubuntu)
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111068 (SMTP/POP3/IMAP Server OS Identification)
Concluded from IMAP banner on port 143/tcp: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED] Dovecot (Ubuntu) ready.
* ID ("name" "Dovecot")
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111068 (SMTP/POP3/IMAP Server OS Identification)
Concluded from POP3 banner on port 995/tcp: +OK Dovecot (Ubuntu) ready.
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111068 (SMTP/POP3/IMAP Server OS Identification)
Concluded from IMAP banner on port 993/tcp: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot (Ubuntu) ready.
* ID ("name" "Dovecot")
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111068 (SMTP/POP3/IMAP Server OS Identification)
Concluded from POP3 banner on port 110/tcp: +OK Dovecot (Ubuntu) ready.

*11 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 25/tcp

NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

*12 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 25/tcp

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_RC4_128_SHA

*13 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 110/tcp

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_RC4_128_SHA

*14 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 995/tcp

'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

*15 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 22/tcp

The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
server_host_key_algorithms:
ssh-rsa,ssh-dss,ecdsa-sha2-nistp256,ssh-ed25519
encryption_algorithms_client_to_server:
aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client:
aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
mac_algorithms_client_to_server:
hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
mac_algorithms_server_to_client:
hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com

*16 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 995/tcp

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_RC4_128_SHA

*17 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 110/tcp

'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

*18 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 25/tcp

'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_AES_128_GCM_SHA256
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA256
TLS_DH_anon_WITH_AES_256_GCM_SHA384
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA

TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA

*19 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 143/tcp

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_RC4_128_SHA

*20 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 993/tcp

'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

*21 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 143/tcp

'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

*22 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - general/tcp

Detected Dovecot
Version: unknown
Location: 143/tcp
CPE: cpe:/a:dovecot:dovecot
Concluded from version/product identification result:
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE
STARTTLS LOGINDISABLED] Dovecot (Ubuntu) ready.
* ID ("name" "Dovecot")
Detection Method: IMAP Banner
Detected Dovecot
Version: unknown
Location: 993/tcp
CPE: cpe:/a:dovecot:dovecot
Concluded from version/product identification result:
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE
AUTH=PLAIN] Dovecot (Ubuntu) ready.
* ID ("name" "Dovecot")
Detection Method: IMAP Banner
Detected Dovecot
Version: unknown
Location: 110/tcp
CPE: cpe:/a:dovecot:dovecot
Concluded from version/product identification result:
+OK Dovecot (Ubuntu) ready.
Detection Method: POP3 Banner
Detected Dovecot
Version: unknown
Location: 995/tcp
CPE: cpe:/a:dovecot:dovecot
Concluded from version/product identification result:
+OK Dovecot (Ubuntu) ready.
Detection Method: POP3 Banner

*23 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 993/tcp

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_RC4_128_SHA

*24 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 143/tcp

'Strong' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the SSLv3 protocol.
No 'Anonymous' cipher suites accepted by this service via the SSLv3 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

*25 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 110/tcp

'Strong' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the SSLv3 protocol.
No 'Anonymous' cipher suites accepted by this service via the SSLv3 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

*26 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 25/tcp

'Strong' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the SSLv3 protocol.
'Anonymous' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA
'Strong' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_AES_128_GCM_SHA256
TLS_DH_anon_WITH_AES_256_CBC_SHA256
TLS_DH_anon_WITH_AES_256_GCM_SHA384
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA

TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_AES_128_GCM_SHA256
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA256
TLS_DH_anon_WITH_AES_256_GCM_SHA384
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA

*27 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 995/tcp

'Strong' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the SSLv3 protocol.
No 'Anonymous' cipher suites accepted by this service via the SSLv3 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

*28 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 993/tcp

'Strong' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the SSLv3 protocol.
No 'Anonymous' cipher suites accepted by this service via the SSLv3 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

*29 Vulnerability Detection Result for Host 38.123.140.31 (demoweb.clone-systems.com) - 25/tcp

'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_AES_128_GCM_SHA256
TLS_DH_anon_WITH_AES_256_CBC_SHA256
TLS_DH_anon_WITH_AES_256_GCM_SHA384
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA