Responsible Disclosure Policy

SOC 2 Criteria: CC2.2, CC5.3

Metomic is committed to ensuring the safety and security of our customers. We aim to foster an open partnership with the security community, and we recognize that the work the community does is important in continuing to ensure safety and security for all of our customers. We have developed this policy to both reflect our corporate values and to uphold our legal responsibility to good-faith security researchers that are providing us with their expertise.

Scope

Metomic's Responsible Disclosure Policy covers the following products:

- Metomic's core platform

We intend to increase our scope as we build capacity and experience with this process. Researchers who submit a vulnerability report to us will be given full credit on our website once the submission has been accepted and validated by our product security team.

Legal Posture

Metomic will not engage in legal action against individuals who submit vulnerability reports through our Vulnerability Reporting inbox. We openly accept reports for the currently listed Metomic products. We agree not to pursue legal action against individuals who:

- Engage in testing of systems/research without harming Metomic or its customers.
- Engage in vulnerability testing within the scope of our vulnerability disclosure program.
- Test on products without affecting customers, or receive permission/consent from customers before engaging in vulnerability testing against their devices/software, etc.
- Adhere to the laws of their location and the location of Metomic. For example, violating laws that would only result in a claim by Metomic (and not a criminal claim) may be acceptable as Metomic is authorizing the activity (reverse engineering or circumventing protective measures) to improve its system.
- Refrain from disclosing vulnerability details to the public before a mutually agreed-upon timeframe expires.

How to Submit a Vulnerability

To submit a vulnerability report to Metomic's Product Security Team, please utilize the following email security@metomic.io

Preference, Prioritization, and Acceptance Criteria

We will use the following criteria to prioritize and triage submissions.

What we would like to see from you:

- Well-written reports in English will have a higher probability of resolution.
- Reports that include proof-of-concept code equip us to better triage.
- Reports that include only crash dumps or other automated tool output may receive lower priority.
- Reports that include products not on the initial scope list may receive lower priority.
- Please include how you found the bug, the impact, and any potential remediation.
- Please include any plans or intentions for public disclosure.

What you can expect from Metomic:

- A timely response to your email (within 5 business days).
- After triage, we will send an expected timeline, and commit to being as transparent as possible about the remediation timeline as well as on issues or challenges that may extend it.
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- Credit after the vulnerability has been validated and fixed.

If we are unable to resolve communication issues or other problems, Metomic may bring in a neutral third party to assist in determining how best to handle the vulnerability.