Date of Last Revision:

Purpose

This policy aims to ensure a consistent and secure manner for persons to communicate suspected vulnerabilities of Zerigo products or services. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to Zerigo.

Scope

This Vulnerability Disclosure policy aims to ensure a consistent and secure manner in which individuals (e.g., security researchers) may communicate suspected vulnerability to Zerigo products or services. Zerigo is committed to continually improving our organization's security and, more specifically, our information assets security. The responsible disclosure of security vulnerabilities helps us ensure the security and privacy of our users.

- This vulnerability disclosure policy applies to any vulnerabilities internal or external parties consider reporting to Zerigo.
- It is recommended to read this vulnerability disclosure policy fully before reporting a vulnerability and always acting in compliance with it.
- Zerigo values and thanks those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

Guidelines

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give permission to act in any manner that is inconsistent with the law, or which might cause the Zerigo or partner organizations to be in breach of any legal obligations. Under this policy, “research” means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability’s presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- Do not submit a high volume of low-quality reports.

Once you’ve established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

ZERIGO
HEALTH

Test methods

A researcher acting in good faith to discover, test and submit vulnerabilities or indicators of vulnerabilities are authorized provided testing activities are limited exclusively to:

- Testing to detect a vulnerability or identify an indicator related to a vulnerability.
- Sharing information with, or receiving information from, us about a vulnerability or an indicator related to a vulnerability.
- Researchers may not harm any system or data on our system or exploit any potential vulnerabilities beyond the minimal amount of testing required to prove that a vulnerability exists or to identify an indicator related to a vulnerability.
- Researchers must not establish command line access and/or persistence; pivot to other systems; escalate privileges; attempt to move laterally within the network; disrupt access to our services; or introduce any malware in the course of testing.
- Researchers must avoid intentionally accessing the content of any communications, data, or information transiting or stored on any of our information systems except to the extent that the information is directly related to a vulnerability and the access is necessary to prove that the vulnerability exists.

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data.
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing.
- Researchers must not intentionally exfiltrate or copy our data, or open, take, or delete files.
- Researchers may not intentionally compromise the privacy or safety of our personnel (e.g. employees or contractors) or any third parties.
- Researchers may not publicly disclose any details of the vulnerability, indicator of vulnerability, or the content of information rendered available by a vulnerability, until that vulnerability is remediated and they receive explicit written authorization from Zerigo.
- Researchers may not intentionally compromise the intellectual property or other commercial or financial interests of any of our personnel or entities or any third parties through their research.

Reporting a vulnerability

If you discover a vulnerability or suspected vulnerability, you must provide a report describing the vulnerability which includes:

- A description of the vulnerability and the potential impact of the vulnerability.
- Product details for the software or hardware that are potentially impacted.
- Step by step instructions on how to reproduce the issue.
- Suggested mitigation or remediation actions, as appropriate.
- Information on how you may be contacted by us.

Please send your report to security@zerigohealth.com

After you have submitted your report, Zerigo's Cybersecurity team will respond to your report within five working days and aim to triage your report within 10 working days. We'll also aim to keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to inquire on the status but avoid doing so more than once every 14 days. This allows our teams to focus on the curative action.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Once your reported vulnerability has been resolved, we welcome requests to disclose your report. Zerigo would like to unify guidance to affected users, and coordinate any public release.