Zimperium Vulnerability Disclosure Policy

Last Revisited: December 04, 2024

ZIMPERIUM®

www.zimperium.com

Zimperium is committed to ensuring the security of its products and of our customers' and end-users' information. 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 us.

This policy describes what systems and types of research are covered under this policy, how to send us vulnerability reports, and how long we ask security researchers to wait before publicly disclosing vulnerabilities.

Zimperium affirms that we will not seek prosecution of any security researcher who reports any security vulnerability on a Zimperium service or system, where the researcher has made a good faith effort to act in accordance with this disclosure policy. We respect the anonymity of researchers reporting vulnerabilities through this policy, disclosing identities only with consent or as legally required. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

Guidelines

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, exfiltration of information, degradation of user experience, disruption to production systems, destruction or manipulation of data, and public disclosure of proprietary code.
- 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**.

Test methods

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

To report a vulnerability

Please provide the following information:

- Product Name and Version: Please specify the exact product and version you encountered the vulnerability in.
- Detailed Description: Clearly describe the vulnerability, including the technical details and potential impact.
- Proof of Concept (PoC): If possible, please provide a PoC to demonstrate the vulnerability. However, please avoid public disclosure of the PoC until we have had a chance to address the issue.
- Contact Information: Provide your email address or other contact information so we can communicate with you effectively.
- Submit your report by sending an email to security.intake@zimperium.com. Encrypt your data using the following PGP Key. If you are unfamiliar, please email us at the same address and request an alternative method.

-----BEGIN PGP PUBLIC KEY BLOCK-----
mDMEZyUpAxYJKwYBBAHaRw8BAQdAQVrda4vHX52syIHGJx/uPTDH/GLMLWaiupVwEnsLG
YW0MIppbXBlcml1bSBTZWN1cml0eSA8c2VjdXJpdHkuaW50YWtlQHppbXBlcml1bS5jb20+iJ
kEExYKAEEWIQT5vsIr4gIBuntmzeXbKEEEWzWYvQUCZyUpAwIbAwUJBaN6jQULCQgHAgIiAgY
VCgkICwIEFgIDAQIeBwIXgAAKCRDbKEEEWzWYvWTjAPsEZGKfibz0bwVitQNqIamghbJ9SoIPI
o9nPhnMW+yOzQD9GHBunqaNmxqI0ppjdvOWp1ULeVQA4wQDnrPJvxnEhQe4OARnJSkDE
gorBgEEAZdVAQUBAQdAlpmssT4KVTKJBgv0lXJGDrr1VNjdOt5mW0dhxa5rACcDAQgHiH4E
GBYKACYWIQT5vsIr4gIBuntmzeXbKEEEWzWYvQUCZyUpAwIbDAUJBaN6jQAKCRDbKEEEWz
WYvSzaAQCKernqBNRIqoWJ+LrIrky5nObJtK6SNLi7O4SSUDjntwEAqZ6DNLTVej8+W0A0YdV
Vt2e6S0IDLXpgceZ+EjfyCAs=
=wbTC
-----END PGP PUBLIC KEY BLOCK-----

Upon receiving your report, we will

- Acknowledge your report promptly.
- Investigate the vulnerability.
- Coordinate with our security team to develop a fix.
- Communicate with you throughout the process.

Please note

- We ask that you refrain from public disclosure of the vulnerability until we have had a chance to address it.
- We will treat your report confidentially and responsibly.
- We may offer rewards or recognition for significant vulnerabilities, which will be issued at the sole discretion of the Zimperium Security Team. (Anonymous submissions, or submission of findings from automated tools without a detailed analysis are ineligible for payment).

Questions

Questions regarding this policy may be sent to security.intake@zimperium.com.
We also invite you to contact us with suggestions for improving this policy.

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244