Vulnerability Disclosure Policy

Introduction

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.

We want security researchers to feel comfortable reporting vulnerabilities they've discovered – as set out in this policy – so we can fix them and keep our users safe. We have developed this policy to reflect our values and uphold our sense of responsibility to security researchers who share their expertise with us in good faith.

Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized, we will work with you to understand and resolve the issue quickly, and Enovix will not recommend or pursue legal action related to your research.

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, 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 command line access and/or persistence, 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.
- You do not intentionally compromise the privacy or safety of Enovix personnel (e.g. civilian employees or military members), or any third parties.
- You do not intentionally compromise the intellectual property or other commercial or financial interests of any Enovix personnel or entities, or any third parties.

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**.

Scope

All systems and services associated with domains listed below are in scope. Likewise, subdomains of each listing, unless explicitly excluded, are always in scope. Additionally, any website published with a link to this policy shall be considered in scope. Vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system or endpoint is in scope or not, contact security@enovix.com before starting your research.

Though we develop and maintain other internet-accessible systems or services, we ask that active research and testing only be conducted on the systems and services covered by the scope of this document. If there is a system not in scope that you think merits testing, please contact us to discuss it first. We may increase the scope of this policy over time.

Domains
enovix.com routejade.com routejade.net

Rules of Engagement

Security researchers must not:

- Test any system other than the systems set forth in the ‘Scope’ section above,
- disclose vulnerability information except as set forth in the ‘Reporting a Vulnerability’ and ‘Disclosure’ sections below,
- engage in physical testing of facilities or resources,
- engage in social engineering,
- send unsolicited electronic mail to Enovix personnel and customers, including “phishing” messages,
- execute or attempt to execute “Denial of Service” or “Resource Exhaustion” attacks,
- introduce malicious software,
- test in a manner which could degrade the operation of Enovix systems; or intentionally impair, disrupt, or disable Enovix systems,
- test third-party applications, websites, or services that integrate with or link to or from Enovix systems,
- delete, alter, share, retain, or destroy Enovix data, or render Enovix data inaccessible, or,
- use an exploit to exfiltrate data, establish command line access, establish a persistent presence on Enovix systems, or “pivot” to other Enovix systems.

Security researchers may:

- View or store Enovix nonpublic data only to the extent necessary to document the presence of a potential vulnerability.

Security researchers must:

- Cease testing and notify us immediately upon discovery of a vulnerability,
- cease testing and notify us immediately upon discovery of an exposure of nonpublic data, and,
- purge any stored Enovix nonpublic data upon reporting a vulnerability.

Reporting a Vulnerability

We accept vulnerability reports by e-mail to security@enovix.com . Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within 3 business days.

What we would like to see from you

In order to help us triage and prioritize submissions, we recommend that your reports:

- Describe the location the vulnerability was discovered and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Be in English, if possible.

What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- Within 3 business days, we will acknowledge that your report has been received.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.

Currently, **we do not offer any monetary compensation for the reported vulnerabilities**.

Disclosure

Enovix is committed to timely correction of vulnerabilities. However, we recognize that public disclosure of a vulnerability in absence of a readily available corrective action likely increases the risk. Accordingly, we require that you refrain from sharing information about discovered vulnerabilities for 90 calendar days after you have received our acknowledgement of receipt of your report. If you believe others should be informed of the vulnerability prior to our implementation of corrective actions, we require that you coordinate in advance with us.

We may share vulnerability reports with the Cybersecurity and Infrastructure Security Agency (CISA), as well as any affected vendors. We will not share names or contact data of security researchers unless given explicit permission.

Questions

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

Content last reviewed January 26, 2024