Coordinated Vulnerability Disclosure Policy

Introduction

Snap One is committed to maintaining its systems' and products' security, privacy, and integrity in compliance with data protection regulations and industry best practices. We recognize the value of external security researchers in helping improve our data security and procedures. Therefore, we encourage the responsible disclosure of security vulnerabilities as outlined below.

This vulnerability disclosure policy applies to external researchers considering reporting vulnerabilities to Snap One. Please read this Vulnerability Disclosure Policy thoroughly before reporting a vulnerability and always act in compliance with this Policy.

Eligibility

- The submitter must agree with our Disclosure Policy.
- The submitter must be the first party/person to disclose an unknown issue responsibly. If we receive submissions on the same issue, we offer recognition to the earliest report for which we received enough actionable information to identify the issue.

Rules of Conduct

- Disclose solely to Snap One in good faith.
- Do not perform vulnerability testing listed as Out of Scope.
- Do not publicly disclose the vulnerability without our consent and review.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Please do not engage in activities that could potentially cause harm to Snap One, our partners, our customers, or our employees.
- 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 or persistence, or "pivot" to other systems.
- Once you have established that a vulnerability exists and before encountering any sensitive data (including personally identifiable information (PII), financial information, proprietary information, or trade secrets), stop your activity, remove related data from your system, and notify us immediately.
- Submit reports with sufficient information to ascertain the vulnerability defined in the Reporting Procedure section.
- Be respectful and professional when interacting with Snap One.

Out of Scope

The following test types are not authorized:

- Denial-of-service attacks
- Physical testing (e.g., office access, open doors)
- Spam or social engineering techniques (e.g., phishing)
- Vulnerability reports from automated tools without an explanation or validation of the issue
- Security issues in third-party systems that integrate with Snap One
- Automated attacks
- Banner Exposure/Version Disclosure

Do not:

- Break any applicable laws or regulations
- Access data
- Modify data in Snap One's systems or services
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities

- Attempt or report any form of denial of service, e.g., overwhelming a service with a high volume of requests
- Disrupt Snap One's services or systems

Reporting Procedure

Submit your report through our secure form on the webpage to report vulnerabilities and ensure confidentiality.

To validate, triage, and prioritize vulnerabilities, ensure your report answers the following questions:

- What type of vulnerability is it?
- What is the target?
- What are the steps to reproduce the vulnerability?
- What tools did you use?
- Who could use the vulnerability, and what would they gain from it?
- Do you have proof-of-concept scripts, logs, or screenshots, and would you share them with us?
- Would you like public recognition for your discovery?
- Do you plan to disclose your report publicly?

Snap One attempts to acknowledge receipt of all submitted reports. Please allow us up to two US business days to respond to your submission. We will provide a reference number for tracking and notify you when remediation has been determined. All vulnerabilities are prioritized based on risk. Vulnerability reports might take some time to triage or address. You are welcome to inquire about the status, but you should only do so once every 45 days to allow the team to focus on the remediation.

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

Once your vulnerability has been resolved, we welcome requests to disclose your report in collaboration with our Legal, Cybersecurity, and Product Teams. We want to unify guidance to affected users, so we will request to review your planned report before publication.

Bounty/Reward

We appreciate the time and effort in our mission to make our products and services secure. We will reward security researchers with a certificate of appreciation on our White Hat Thank You page to express our gratitude for the valid vulnerabilities disclosed. We do not provide a monetary reward for vulnerability reports.

Safe Harbor

Snap One will not seek civil action or initiate a complaint to law enforcement against any security researcher who reports in good faith and follows the terms of this Policy.

We consider activities covered in this Policy to constitute "authorized" conduct under the Computer Fraud and Abuse Act (CFAA) and the Digital Millennium Copyright Act (DMCA), as well as under similar international laws with equivalent concepts. Likewise, if you comply fully with the Policy, we will not bring a DMCA claim against you for circumventing the technological measures we have used to protect the applications in our vulnerability disclosure program scope.

We reserve the right to determine whether any violation of this Policy is accidental or in good faith, and proactive contact with us before any action is a significant factor in that decision. Please submit a report to our secure form before engaging in conduct that may be inconsistent or unaddressed by this Policy.