STAR Labs SG Pte. Ltd.
Vulnerability Disclosure Policy

The goals of the STAR Labs SG Pte. Ltd. ("STAR Labs") Vulnerability Disclosure Policy are two-fold:

1. Protect end users in a timely manner by ensuring that the vendor is acting promptly on the information provided to resolve the issue; and
2. Ensure that the action is as comprehensive as possible, such that it will fix the vulnerability thoroughly without causing further risks to the end users.

Once a vulnerability in a third-party product has been discovered, STAR Labs will:

- Attempt to notify the vendor as soon as practicable via its public vulnerability disclosure contact email or form;
- Provide adequate information in the suspected vulnerability report;
- Assign a Common Vulnerabilities and Exposures ID (CVE ID) to the vulnerability if it is not covered by another CVE Numbering Authority; and
- Publish the CVE and other relevant information on STAR Labs's Advisories page and the CVE List after the vulnerability has been patched/mitigated

STAR Labs will attempt to work with any vendor on reasonable adjustments to the above timeline if there are extenuating circumstances necessitating such adjustments.

Purpose

This policy sets forth the reporting and disclosure process that STAR Labs follow when we discover security vulnerabilities in any products.

Policy

This policy must clearly state the timeline, actions, and responsibilities equally available to all vendors.

Vendor Vulnerability Reporting and Disclosure

If a vulnerability is found in a vendor's product or service, STAR Labs will attempt to contact the vendor by email to notify the vendor of such discovery. STAR Labs will initially attempt to create a secure communication channel with the vendor by exchanging PGP keys for encrypted email. If a secure communication channel is successfully created, then an encrypted copy of the vulnerability report will be sent to the vendor through that channel. If no response to the attempt to create a secure communication channel is received by STAR Labs within nine (9) days, then a description of the vulnerability will be sent by email to the vendor in plain text.

If STAR Labs discovers a vulnerability in a vendor's product or service, it will take the following steps:

Actions to be Taken by STAR Labs	
Day 0	• Initial vendor contact • Assignment of CVE (Common Vulnerabilities and Exposures) if vendor is not a CNA (CVE Numbering Authority) • Vendor name and report date listed on STAR Labs vulnerability tracker website
Day 9	• Second vendor contact if there is no response to STAR Labs's initial communication
Day 45	• Reminder email sent to the vendor with the release date of the vulnerability report
Day 60	• If the vendor has not responded or has stopped responding, a final reminder email will be sent
Day 90	• Email sent to vendor to check if they need extension
Day 120	• Disclosure of the full vulnerability report on the STAR Labs advisories page; however, if the vendor releases a patch or mitigation for the vulnerability before the 120th day, then STAR Labs will disclose the full vulnerability report immediately following vendor's release of such patch or mitigation • CVE publication request submitted to MITRE

At any stage of this process, STAR Labs SG Pte. Ltd. is fully committed to working with vendors to ensure that the technical details and severity of a reported security issue are fully understood. This is accomplished by sharing with the vendor technical information gathered through the research and - when possible - a reliable way to reproduce the issue.
In the interest of fostering coordinated vulnerability disclosure, STAR Labs will attempt to work with any vendor on reasonable adjustments to the above timeline if progress is being made and the 120-day default timeline is not adequate for creating a patch or other type of mitigation that addresses the vulnerability. Extenuating circumstances may result in adjustments to the disclosures and timelines when reasonably necessary.

STAR Labs SG Pte. Ltd.

Protecting users against the ever-evolving threat of cyber attacks

STAR Labs SG Pte. Ltd. accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.