STAR Labs SG Pte. Ltd.
Vulnerability Disclosure Policy

The goals of the STAR Labs SG Pte. Ltd. (“STAR Labs SG Pte. Ltd.”) 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 SG Pte. 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 SG Pte.’s Advisories page and the CVE List after the vulnerability has been patched/mitigated

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

Policy

Once a security issue is found the following steps will be taken by STAR Labs SG Pte. Ltd. to notify the respective parties to fix it.

- Once we have confirmed the vulnerability, we will gather all the necessary information to communicate the details to the affected party.
- STAR Labs SG Pte. Ltd. will try to establish initial contact with the affected vendor via email regarding the vulnerability with all the supporting documents.
- If we don't receive a response from the vendor within seven days of sending the mail, another reminder will be sent. If the vendor did not respond to the reminder, a second reminder will be sent. If the vendor refuses to acknowledge the vulnerability within 30 business days from initial contact, STAR Labs SG Pte. Ltd. will publicly disclose the vulnerability.
- The vulnerability will be disclosed immediately following the vendor's patch or fix release.
- If a fix is not provided within 180 days and no response is received from the vendor, then we will go ahead and disclose the vulnerability.
- In the event that the vendor is unable to provide a fix within 180 days, but has communicated with STAR Labs SG Pte. Ltd. regarding the fix, then the deadline could be adjusted. A maximum of ten months of coordination will be given to the vendor for fixing the vulnerabilities. After that, the vendor will be informed and the vulnerability will be disclosed regardless of the fix.
- The 180-day deadline mentioned above is not a hard deadline. STAR Labs SG Pte. Ltd. can lengthen the deadline. STAR Labs SG Pte. Ltd. is aware that some vulnerabilities can have profound ramifications on the affected systems. For this reason and on a case-by-case basis, STAR Labs SG Pte. Ltd. is open to discussing a timeline extension.
- Until the completion of the disclosure process, STAR Labs SG Pte. Ltd. will maintain the confidentiality of any communication to and from the vendor.
- All the CVEs assigned by STAR Labs SG Pte. Ltd. and its vulnerability disclosures can be found in the STAR Labs SG Pte. Ltd. security advisory. Only the advisories present in the security advisory will be considered as official documents.

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.