Kalkitech

Kalkitech Cybersecurity Vulnerability Management Policy

Kalkitech has put in place a formal Policy (this document) and operational mechanisms to handle the management of cybersecurity vulnerabilities detected in its Software products and offerings, to manage the risks arising thereof. Software in this context applies to a broad range of computer programs including application software, operating system software, embedded firmware, drivers, open source packages, libraries and scripts.

This Policy applies to cybersecurity vulnerabilities that may be detected from the following sources:

a. A Vulnerability Report filed by an external party informing Kalkitech of a security issue or weakness detected in a Kalkitech software offering;
b. A public disclosure of a software vulnerability that may have an impact on Kalkitech software that includes the affected library or module;
c. An internally detected vulnerability – detected by development and or testing teams within Kalkitech

Vulnerability Reporting

Kalkitech encourages any party detecting a security vulnerability in Kalkitech software products to report the issue to us by sending an email to us at secure@kalkitech.com. If you plan to submit sensitive information to us, please send it encrypted using our PGP public key. Instructions on download of the key can be found on the Cybersecurity page on both the ASE and Kalkitech websites.

The Kalkitech's Security Response Team (SRT) monitors all security related communique and is a special team designated to handle detected and reported vulnerabilities. Alternately or additionally, the reporter may also directly submit the report to ICS-CERT, CERT-IN or any other national CERT body designated to handle security vulnerabilities.

When a vulnerability is detected internally within Kalkitech, the SRT shall decide if the vulnerability is to be reported to ICS-CERT (or other CERT bodies) based on the vulnerability score and its impact on the installed base of affected products. The criteria for escalating detected vulnerabilities to CERT is described further below in this policy.

When reporting to Kalkitech SRT, the reporting entity has to indicate if it does NOT wish to remain anonymous, in which case Kalkitech advisories when and if issued, related to the reported incident, shall credit the reporter.

Software Security Vulnerability Phases

A software vulnerability detected in Kalkitech software offerings and reported to the SRT shall pass through the following phases

1. Report Acknowledgement – 2 business days
2. Initial Analysis – 5 business days
3. Investigation – 10 business days
4. Remediation
5. Notification

1. Report Acknowledgement

This phase is triggered when a vulnerability report is received by the SRT. The vulnerability is recorded in a dedicated folder with name, date and time. An authorized member of the SRT acknowledges the receipt of the report (usually within 2 business days) to the reporting entity. The acknowledgement does not presume to confirm or deny the vulnerability but serves as an acknowledgement that the report has been received.

Actions and Artifacts

a. A dedicated repository is created for the reported vulnerability with a running serial ID code assigned by the SRT.
b. An email acknowledgement is sent to the reporting entity containing:
   i. The vulnerability ID assigned
   ii. The contact details including name and email-id of an authorized member of the SRT

2. Initial Analysis

The SRT conducts an analysis of the reported information. The severity and impact of the vulnerability is calculated using CVSS V2 (Common Vulnerability Scoring System). The phase ends with an update to the reporting entity with the analysis results including the CVSS scores and vector. If the CVSS scores satisfy the following criteria, this phase also includes a report to ICS-CERT/CERT-IN. The SRT also identifies the list of Kalkitech products and versions affected by the vulnerability. This phase is expected to conclude within 5 business days.

2.1 Criteria for escalating report to ICS-CERT

A vulnerability that results in a score of 6.85 or higher is required to be reported to ICS-CERT and/or CERT-IN.

Actions and Artifacts

a. The CVSS scoring report is added to the vulnerability repository containing the analysis, the scores and the vector
b. List of Kalkitech products with version numbers affected by the vulnerability
c. Email update is sent with the CVSS report to the reporting entity
d. CVSS report is analyzed against the criteria listed in section 2.1 of this policy and if found meeting the criteria, the vulnerability report is notified to ICS-CERT/CERT-IN

3. Investigation

This phase includes a detailed analysis of the reported vulnerability, including efforts to reproduce the vulnerability. Based upon the analysis, a tentative list of remedies and/or workarounds is created. In this phase SRT also works with other internal departments to identify a list of third parties including customers that may have received products identified in the list of affected products and versions. This phase is expected to conclude within 10 business days.

Actions and Artifacts

a. Detailed documentation on the reported vulnerability
b. Documented Test Cases to reproduce the vulnerability
c. Tentative list of workarounds or remedies with instructions
d. Identification of third parties including customers that may be affected
e. Update to the reporting entity and government organizations that were notified, if applicable
f. Email to affected customers providing a link to access information about the vulnerability. The email contains only an intimation that a vulnerability is detected and names the products affected. Additional information including CVSS report and workarounds are accessible through support section of www.kalkitech.com.

4. **Remediation**

In this phase the SRT works with other departments internally to supervise the development of a remedy to eliminate the vulnerability. This also includes identification of other mitigations and work arounds.

Actions and Artifacts

a. Developed patch, upgrade or software fix to nullify the vulnerability
b. Document on application of the remedy
c. Document on alternative mitigations or workarounds
d. Re-evaluated CVSS score based on observations during the remediation phase
e. Update to the reporting entity and government organizations that were notified, if applicable.

5. **Notification**

This phase marks the conclusion of the vulnerability case and produces an advisory for public consumption. The advisory includes the vulnerability analysis report, credits the reporting entity (if explicitly permitted by the reporting entity), the means to receive the patch/upgrade/fix and the documentation on application of the fix and other workarounds. The advisory is sent to the reporting entity and government organizations if notified. Additionally, the advisory is published on Kalkitech's website in the appropriate section. The list of third parties (customers and others) affected by the vulnerability is notified about the solution.

Actions and Artifacts

a. Detailed Security Advisory prepared and issued by the SRT
b. Advisory sent to the reporting entity and government organizations as applicable
c. Security Advisory published on Kalkitech website(s)
d. Advisory sent to official contacts for affected third parties

SRT Case Conclusion

The SRT initiates a conclusion meeting with internal departments that can benefit from the findings related to the detected vulnerability and presents the highlights of the advisory. The meeting discusses process changes and other measures that may help in preventing the occurrence of similar vulnerabilities across the Kalkitech products domain. The meeting minutes are retained in the Vulnerability repository.