Embever's Software Vulnerability Handling Policy

Published security advisories and contact information can be found on the Embever Cyber Security website:
https://www.embever.com/cybersecurity

Embever recognizes cybersecurity as a critical priority and is dedicated to delivering products, systems, and services that proactively address security needs. Timely and effective management of software vulnerabilities plays a vital role in helping our customers reduce cybersecurity risks. To support this, Embever has implemented a formal vulnerability handling policy, detailed in this document.

The Embever Software Vulnerability Handling Policy applies in the following events:

- An external party (e.g., customer, researcher, government organization) reports a potential vulnerability affecting an Embever solution.
- A vulnerability is publicly disclosed affecting an Embever solution.
- A vulnerability is discovered internally that impacts the installed base.
- Malware targets Embever solutions.

Reporting a vulnerability to Embever

A vulnerability is defined by Embever as a weakness in the computational logic of one of its solutions, found in software and hardware components, that, when exploited, results in a negative impact on confidentiality, integrity, or availability.

While Embever will respond to reports of such vulnerabilities, weaknesses in existing customer installations due to their individual designs or compromised access credentials are not considered vulnerabilities.

Anyone discovering a software vulnerability affecting an Embever solution is encouraged to contact Embever directly.

Reports can be submitted directly to Embever’s Cyber Security Response Team (CERT) using the email:
cybersecurity@embever.com

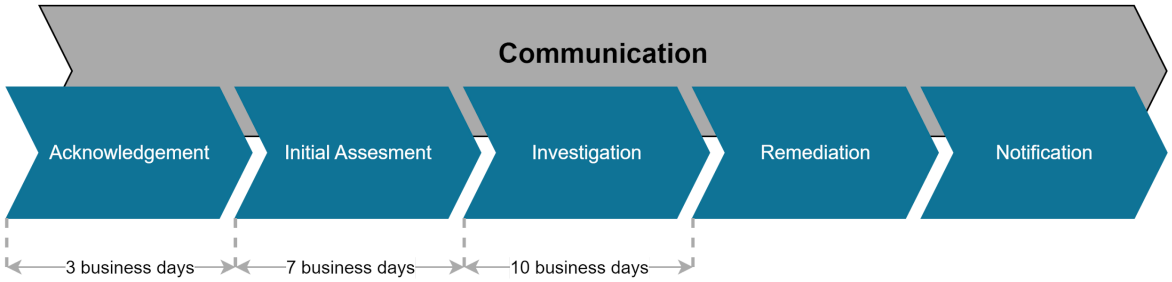
Embever recommends using PGP to securely transmit sensitive data. The public PGP key for Embever’s Cyber Security Response Team can be found:

- On the Embever Cyber Security website under "PGP key for secure reporting", or
- Directly via this link: Public PGP Key for Embever Cybersecurity Response Team

---

The Embever Software Vulnerability Handling Policy

Embever's software vulnerability handling policy defines five phases. Each phase takes input from the previous phase and has clearly defined deliverables. A debriefing is performed at the closure of each case to review and improve the policy and processes.



1. First Response

We acknowledge the receipt of the vulnerability report within 2 business days and establish a secure communication channel with the reporting party. At this stage, a dedicated team lead is assigned to oversee the handling of the vulnerability and to communicate with relevant stakeholders throughout the process.

2. Preliminary Assessment

In this stage, we verify the validity of the reported vulnerability, assess its severity using the Common Vulnerability Scoring System (CVSS), and involve any necessary parties for a coordinated response. This initial assessment, typically completed within 7 business days, includes creating documentation for the vulnerability, assigning a severity rating, and identifying potentially affected products and versions. Periodic updates are provided to the reporting entity and any other involved parties.

3. Investigation

We conduct a detailed analysis of the vulnerability, working closely with the reporting entity and any relevant third parties, such as software suppliers, to reproduce the issue and document it thoroughly. This phase includes preparing for the remediation stage and is usually completed within 10 business days. Documentation is updated with findings, and test cases are created to confirm the vulnerability's presence. The reporting entity and involved parties receive periodic updates during this phase.

4. Remediation

Our team develops and validates a solution to address the vulnerability, whether through software fixes or mitigation measures. We continuously reassess the severity of the vulnerability, especially if new information becomes available. Remediation may involve configuration changes or recommended security practices, and we aim to provide alternatives when possible to help customers avoid immediate disruptions. Updates are shared with the reporting entity and other relevant parties, who may also be asked to verify the solution's effectiveness.

5. Notification

In the final stage, we prepare and release a vulnerability security advisory to communicate the resolution. This advisory includes all necessary details about the vulnerability, affected products, and mitigation steps. We close the vulnerability handling process by issuing final updates to the reporting entity and any other involved stakeholders, ensuring all parties are informed and any residual risks are minimized.