Hitachi ABB Power Grids Approach to Software Vulnerability Handling

Published security advisories and contact information can be found on the Hitachi ABB Power Grids Cybersecurity web page at https://www.hitachiabb-powergrids.com/cybersecurity

Disclaimer

Purpose

Hitachi ABB Power Grids has identified cybersecurity as a key requirement and is committed to providing customers with products, systems and services that clearly address cybersecurity. Proper and timely handling of software vulnerabilities is one important factor in helping customers minimize risks associated with cybersecurity. Hitachi ABB Power Grids has therefore established a formal vulnerability handling policy which is described in this document.

The Hitachi ABB Power Grids Software Vulnerability Handling Policy will be applied at least in the following events:

- An external party (e.g. customer, researcher, government organization) approaching Hitachi ABB Power Grids reporting a potential vulnerability affecting a Hitachi ABB Power Grids solution
- A vulnerability disclosed publicly affecting a Hitachi ABB Power Grids solution
- A vulnerability being discovered internally that impacts the installed base
- Malware targeting Hitachi ABB Power Grids solutions

Reporting a vulnerability to Hitachi ABB Power Grids

In Hitachi ABB Power Grids' view, a vulnerability is a weakness in the computational logic of one of Hitachi ABB Power Grids solutions found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability.

While Hitachi ABB Power Grids will also of course react to reports of such occurrences, weaknesses in existing customer installation due to their individual designs, or compromised access credentials are not considered a vulnerability.

Anyone discovering a software vulnerability affecting a Hitachi ABB Power Grids solution is encouraged to contact Hitachi ABB Power Grids directly. Reports can be submitted directly to Hitachi ABB Power Grids Security Incident Readiness Team (PG SIRT), using the E-Mail address: cybersecurity@hitachi-powergrids.com

In the event someone discovering a vulnerability relating to a Hitachi ABB Power Grids solution does not wish to directly contact or interact with Hitachi ABB Power Grids, we recommend contacting the United States CISA US-CERT (https://us-cert.cisa.gov/ics), or any other national CERT or other recognized coordinating organization.

Hitachi ABB Power Grids recommends the use of PGP to securely transmit any sensitive data. The public PGP key for PG SIRT can be found on the Cybersecurity web page at https://www.hitachiabb-powergrids.com/cybersecurity under the sections "*Report an Incident or Vulnerability*".

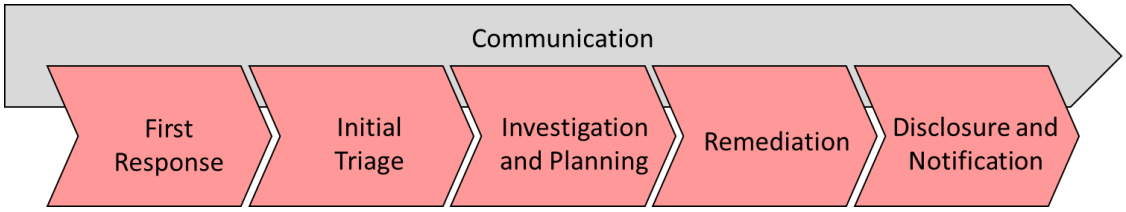
The report should include, if possible, the affected Hitachi ABB Power Grids solution, a description of the vulnerability, and where applicable additional information such as evidence or proof of concept, whether the vulnerability has been already published in another way, and whether the reporter is committed to coordinated disclosure.

If the reporting entity does not wish to stay anonymous, Hitachi ABB Power Grids will acknowledge the reporting entity with the discovery of the vulnerability, e.g. as part of official Hitachi ABB Power Grids advisories issued based on the reported vulnerability.

The Hitachi ABB Power Grids software vulnerability handling policy

Hitachi ABB Power Grids' software vulnerability handling policy defines five phases. Each phase takes input from the previous phase and has clearly defined deliverables.

In addition to these five phases a debriefing is performed at the closure of each vulnerability case to review and improve the policy and the supporting processes.



First Response

Objective
Formal acknowledgment of the information received and establishment of secure communication channel between Hitachi ABB Power Grids and the reporting entities.

At this point an official Hitachi ABB Power Grids lead is assigned to handle the vulnerability.

Deliverables
Written acknowledgment to the reporting entities by E-Mail including the name and contact information of the Hitachi ABB Power Grids lead within 7 calendar days.

Initial Triage

Objective
Verification of the validity of the reported vulnerability, first severity and impact assessment (using Common Vulnerability Scoring System v3[1]), involvement of government organizations or other third parties as necessary and coordination of further steps between all involved parties.

Deliverables

- First documentation of the vulnerability including unique identifier, first severity rating, and list of potentially affected products and versions.
- Periodic update to reporting entities, involved government organizations and third parties.

Investigation

Objective
Detailed documentation of the vulnerability in collaboration with reporting entities and reproduction of the vulnerability. Involvement of potentially affected 3rd parties (e.g. 3rd party software suppliers). Preparation and planning for remediation and notification phases.

Escalation to Hitachi ABB Power Grids companywide level if the vulnerability affects multiple Hitachi ABB Power Grids products.

[1] https://www.first.org/cvss

Deliverables

- Detailed documentation of vulnerability and affected products.
- Test case(s) to verify existence of vulnerability.
- Periodic update to reporting entities, involved government organizations and third parties.

Remediation

Objective

Development and validation of software remediation and / or mitigations. Continuous reassessment of severity to e.g. account for changes in publicly available information.

Deliverables

- Validated software remediation
- Validated mitigations, which can include configuration changes (e.g. disabling of vulnerable service) or recommendations on deployment and configuration of security solutions (e.g. firewalls). It is Hitachi ABB Power Grid's goal to provide mitigations if possible to offer customers alternatives to updating a running product immediately. Depending on the severity of the vulnerability and the time needed to develop a software remediation the alternative mitigations might be communicated before the final software remediation is available.
- Periodic update to reporting entities, involved government organizations and third parties.

Hitachi ABB Power Grids might approach the reporting entities or government organizations to verify that the software remediation eliminates the vulnerability and that the proposed mitigation alternatives properly address the vulnerability and reduce the risk significantly.

Notification

Objective

Development and dissemination of vulnerability security advisory. Closure of the vulnerability handling process.

Deliverables

- Final update to reporting entities, involved government organizations and third parties.
- Official vulnerability security advisory