ABB DOC ID: 9ADB005059
REVISION: E
DATE: 2019-03-22

ABB’s approach to software vulnerability handling

Published security advisories and contact information can be found on the ABB Cyber Security portal https://www.abb.com/cybersecurity.

Disclaimer

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB provides no warranty, express or implied, for the information contained in this document, and assumes no responsibility for the information contained in this document or for any errors that may appear in this document.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

Purpose

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

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

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

Reporting a vulnerability to ABB

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

While ABB 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 an ABB solution is encouraged to contact ABB directly, or alternatively any national CERT or other coordinating organization.

Reports can be submitted directly to ABB's Cyber Security Response Team, which acts as the official ABB CERT, using the email address: cybersecurity@ch.abb.com

ABB recommends the use of PGP to securely transmit any sensitive data. The public PGP key for ABB's Cyber Security Response Team can be found on the ABB Cyber Security portal https://www.abb.com/cybersecurity under the sections "Alerts and Notifications" and then "Report a vulnerability" or directly by following this link: Public PGP Key for ABB Cyber Security Response Team.

In case that someone discovering a vulnerability relating to an ABB solution does not wish to directly contact or interact with ABB we recommend contacting ICS-CERT (https://ics-cert.us-cert.gov), any other national CERT or other coordinating organization.

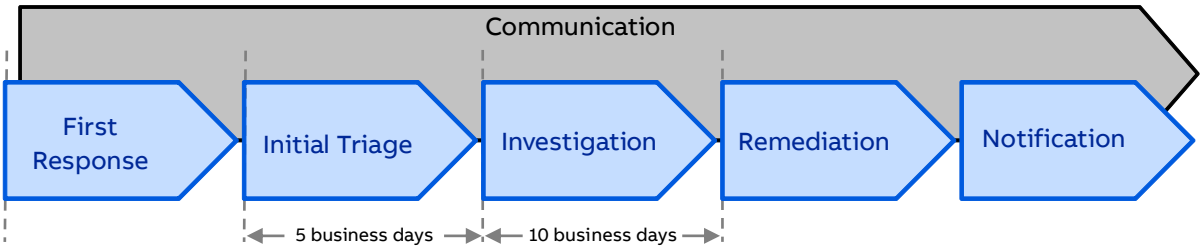
If the reporting entity does not wish to stay anonymous ABB will acknowledge the reporting entity with the discovery of the vulnerability, e.g. as part of official ABB advisories issued based on the reported vulnerability.

The report should include, if possible, the affected ABB 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.

The ABB software vulnerability handling policy

ABB's 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 (usually within 2 business days) of the information received and establishment of secure communication channel between ABB and the reporting entities.

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

Deliverables
Written acknowledgment to the reporting entities by email or paper letter including the name and contact information of the ABB lead.

Initial Triage

Objective
Verification of the validity of the reported vulnerability, first severity and impact assessment (using Common Vulnerability Scoring System[1]), involvement of government organizations or other third parties as necessary and coordination of further steps between all involved parties. Completion usually within 5 business days.

Following the verification, CVE(s) will be assigned using MITRE's CNT2.2[2] rules.

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.

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

[2] https://cve.mitre.org/cve/cna/rules.html#Appendix_C

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. Completion usually within 10 business days.

Escalation to ABB Group level if the vulnerability affects multiple ABB products.

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 public available information.

Deliverables

- Validated software remediation
- Validated mitigations: can include configuration changes (e.g. disabling of vulnerable service) or recommendations on deployment and configuration of security solutions (e.g. firewalls). It is ABB'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.

ABB might approach the reporting entities or government organizations to verify that the software remediation actually 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