# Schneider Electric Vulnerability Handling & Coordinated Disclosure Policy

V3.0
Prepared By: SE Corporate Product CERT
Date: July 19, 2022

# Schneider Electric Vulnerability Handling & Coordinated Disclosure Policy

Schneider Electric's Vulnerability Handling & Coordinated Disclosure Policy ("Policy") addresses cybersecurity vulnerabilities affecting Schneider Electric products, software, and systems to support the security and safety of our customers. We work collaboratively with researchers, Cyber Emergency Response Teams (CERTs), and asset owners to ensure that accurate information is provided in a timely fashion to adequately protect customer installations. This policy targets compliance with ISO/IEC 29147 and ISO/IEC 30111. Schneider Electric values the work of security researchers and seeks to work collaboratively and responsibly with them to improve the security of its products, software, and systems. To that end, Schneider Electric operates a coordinated disclosure program through its Corporate Product CERT (CPCERT). Researchers participating in this program agree to follow responsible research and disclosure principles, and the program rules described below. In performing research on Schneider Electric products, software, and systems and participating in this program, researchers agree:

- Not to cause any harm to product owners or operators, Schneider Electric, or other third parties, including by compromising installed products, software, and systems or the privacy of Schneider Electric customers, employees, or third parties;
- To comply with applicable governing law; and
- That any disclosure of a reported vulnerability shall be conducted according to the terms of this program.

Schneider Electric agrees not to pursue legal action relating to a vulnerability report and the associated security research against a researcher that complies with the program rules.

### 1. Report a Vulnerability

To report a security vulnerability affecting a Schneider Electric product, refer to our Report a Vulnerability page. There you will find all the information necessary to report a vulnerability. Schneider Electric CPCERT usually responds to incoming reports within two business days. (Reference: United States Eastern Time)

Include the following information in an encrypted report using our PGP key:

- Product name, model, and firmware version. Include product reference ID and/or part number if available
- Any special configuration required to reproduce the issue
- Step-by-step instructions to reproduce the issue
- Proof-of-concept or exploit code
- Impact of the issue, including how an attacker could exploit the issue
- Any other relevant information

## 2. Evaluation

Schneider Electric will analyze the reported potential vulnerability. The CPCERT will communicate to the reporting entity our conclusion and/or a request for more information upon completion of review of the potential vulnerability, as determined in its sole discretion. Reporting entities must respond within 30 days or the case will be closed.

If Schneider Electric determines that a report does not identify a vulnerability or that the reported vulnerability is a duplicate of a previously reported vulnerability, it will notify the reporting entity.

Note: The time required for handling, including Mitigation and Disclosure, may be impacted by the relative criticality of the vulnerability and other relevant factors.

## 3. Mitigation

Schneider Electric determines the root cause of the vulnerability and develops a resolution or determines mitigation measures. During this phase, the CPCERT maintains active and secure communications with the reporting entity regarding any mitigations, potentially including advisories, patches, or updates.

## 4. Disclosure

Schneider Electric discloses vulnerabilities and associated risk mitigation measures to support customers as they secure installed products, software, and systems.

Schneider Electric typically discloses reported vulnerabilities rated Medium, High, or Critical through a Security Notification posted on Schneider Electric's Cybersecurity Support Portal. A Security Notification is intended to provide customers with sufficient information to understand the vulnerability and take appropriate mitigating actions. Each Security Notification contains, as appropriate:

- Overall description of the vulnerability including CVSS score, impact of the vulnerability if exploited, and CVE (if applicable).
- Identification of products, software, and systems and versions affected.
- Patches or mitigating actions to reduce the risk of exploit, including patch download instructions where applicable. Schneider Electric always encourages customers to take advantage of these updates and/or instructions and patch their installations appropriately.

Schneider Electric assigns a Common Vulnerabilities and Exposures or CVE number (Schneider Electric is a CVE Numbering Authority in association with MITRE) to any reported vulnerability that relates to a currently supported product and will be disclosed in a Security Notification. With the consent of the reporting entity, Schneider Electric will acknowledge the researcher for the discovery of a vulnerability in the relevant Security Notification and also on the Schneider Electric Wall of Thanks, which acknowledges researchers for their contributions. Schneider Electric reserves the right not to acknowledge any researcher who does not adhere to the terms of this Policy.

Security Notifications are published on the Schneider Electric corporate website on the second Tuesday of each month.

Schneider Electric discloses reported vulnerabilities rated as Low through Version Release Notes. Version Release Notes will include a short summary of the general nature of vulnerabilities addressed in the release but will not include more detailed information. Schneider Electric typically does not assign a CVE number to any vulnerability rated as Low.

All released Schneider Electric offers shall be considered under the Coordinated Vulnerability Disclosure process. Schneider Electric evaluates vulnerability reports relating to products, software, and systems that are no longer supported on a case-by-case basis. Schneider Electric will provide a Security Notification or reference in Version Release Notes for such vulnerabilities at its discretion.

## 5. Disclosure Coordination

Reporting entities may not disclose any potential vulnerability reported through this program prior to the issuance of an associated Security Notification or Version Release Notes. If the vulnerability is expected to impact other vendors, then CPCERT can engage an external coordinator to coordinate public release of advisories and facilitate collaboration among the participating entities. After such coordinated disclosure, reporting entities may further disclose or publicize their role in identifying the vulnerability, but may not disclose further details about their engagement with Schneider Electric (including electronic communications), the vulnerability, or associated exploit steps without the express prior written consent of Schneider Electric. Researchers are required to adhere to this policy to reduce risk to customers of Schneider Electric.

## 6. Miscellaneous

By submitting a vulnerability report to Schneider Electric, a Researcher grants Schneider Electric a non-exclusive worldwide, irrevocable, perpetual, sub-licensable royalty-free license to any intellectual property contained in that report or any follow up communications related to the report to analyze, commercialize, publicize, disclose, or otherwise use such intellectual property in any manner. Participating in this program does not give a Researcher any right to any intellectual property of Schneider Electric.

Schneider Electric reserves the right to change these terms at any time and without advance notice. Continued participation in this program after a change in terms constitutes acceptance of the amended terms.

Reporting entities subject to this policy are required to fully cooperate with any requests by Schneider Electric for additional information, assistance, research, and agree to coordinate disclosures of any vulnerabilities as noted herein and as may be requested by Schneider Electric in its sole discretion.

## How to Contact Schneider Electric’s Corporate Product CERT:

**Website:** https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp
**Email:** cybersecurity@se.com

**PGP Key Information:**
CPCERT 2016-01-11
Key ID: 0x01573082
Fingerprint: 419A A83D 2244 2371 1A1D FD59 A515 9D04 0157 3082
https://keyserver.pgp.com/vkd/SubmitSearch.event?SearchCriteria=cybersecurity%40schneider-electric.com

**Download PGP Key:**
https://keyserver.pgp.com/vkd/DownloadKey.event?keyid=0xA5159D0401573082

**Revision Control:**

| | |
|---|---|
| Version 1.0<br>*28 January 2019* | Original Release |
| Version 2.0<br>*05 April 2019* | Updates to reporting a vulnerability process, and frequency of disclosures |
| Version 2.1<br>*18 November 2019* | Updates to evaluation and disclosure section |
| Version 3.0<br>*19 July 2022* | Updates to overview, disclosure, and disclosure coordination sections |

Product Security Office

Digitally signed by Product Security Office
Date: 2022.07.19 19:09:26 -04'00'