Schneider Electric Vulnerability Management Policy

Schneider Electric’s vulnerability management policy addresses cybersecurity vulnerabilities affecting Schneider Electric products in order 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. Schneider Electric’s Corporate Product CERT (CPCERT) is responsible for managing and alerting on vulnerabilities and mitigations affecting products.

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. Reporting entities must respond within 30 days or the case will be closed.

If Schneider Electric determines that a reported vulnerability is valid, Schneider Electric will then assess the risk to customers, products affected, field population, and severity of the vulnerability. Note: The time required for handling, including Mitigation and Disclosure, may be impacted by the relative criticality of the vulnerability.

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

Once a mitigation is available, Schneider Electric will prepare and release a security notification. General security notifications are published on the Schneider Electric corporate website on the second Tuesday of each month, unless the notification is limited to a specific group of customers, in which case customers may be contacted directly to support remediation.

During the disclosure phase, Schneider Electric assigns a Common Vulnerabilities and Exposures or CVE number (Schneider Electric is a CVE Numbering Authority in association with MITRE). With the consent of the reporting entity, Schneider Electric will acknowledge the researcher for their discovery in our security notification.

Reporting entities are required to adhere to this policy in order to provide our customers the time they need to protect their installations and operations through defined mitigation strategies. Schneider Electric reserves the right to withhold acknowledgement at its sole discretion in the event of an uncoordinated disclosure or if a reporting entity fails to support Schneider Electric or adhere to this policy.

For reports regarding products that are no longer supported, Schneider Electric will evaluate CVE assignment and discovery acknowledgement on a case-by-case basis.

Each disclosure will also contain:

- Overall description of the vulnerability including CVSS score, impact of the vulnerability if exploited, and CVE (if applicable).
- Identification of products 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.

How to Contact Schneider Electric’s Corporate Product CERT:

Website: http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

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:

<table>
<thead>
<tr>
<th>Version 1</th>
<th>Original Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>28 January 2019</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version 2</th>
<th>Updates to reporting a vulnerability process, and frequency of disclosures</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 April 2019</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version 2.1</th>
<th>Updates to evaluation and disclosure section</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 November 2019</td>
<td></td>
</tr>
</tbody>
</table>

Product Security Office

Digitally signed by Product Security Office
Date: 2019.11.18 12:18:34 -05'00'