Life Is On | Schneider Electric

Schneider Electric Vulnerability Management Policy

V 2.0
Prepared By : SE Corporate Product CERT
Date: April 5, 2019

Schneider Electric Vulnerability Management Policy

Schneider Electric's vulnerability management policy addresses cybersecurity vulnerabilities affecting Schneider Electric products and systems in order to support the security and safety of our installed solutions, protecting our customers and the environment. 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 their installations. Schneider Electric's Corporate Product CERT (CPCERT) is responsible for managing and alerting on vulnerabilities and mitigations affecting products and solutions.

1. Report a Vulnerability

To report a security vulnerability affecting a Schneider Electric* product or solution please refer to our Report a Vulnerability page, there you will find all the information necessary to responsibly disclose. Schneider Electric CPCERT usually responds to incoming reports within two business days. (Reference: United States EST)

Please 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

Schneider Electric strongly encourages reporting of all product or system vulnerabilities, regardless of where a product is in its lifecycle. We value all such information and the confidentiality of the reporting entity. We will maintain active and secure communications with the reporting entity and coordinate the disclosure to best protect our customer's, the public, and the environment. We encourage reporting entities to support our disclosure policy so as to provide customer's adequate time to protect their systems with the mitigation strategies we define.

** Please note the Schneider Electric industrial software business and AVEVA have merged to trade as AVEVA Group plc, a UK listed company. The Schneider Electric and Life is On trademarks are owned by Schneider Electric and are being licensed to AVEVA by Schneider Electric. For information on how to reach AVEVA support for your product, please refer to this link: AVEVA Software Global Customer Support for any cybersecurity needs and visit https://sw.aveva.com/support/cyber-security-updates or cybersecurity bulletins and information. For a list of products that will be managed by the AVEVA cybersecurity team please reference the AVEVA and Schneider Electric Deal document.*

2. Evaluation

Schneider Electric will analyze the potential vulnerability. The CPCERT will report back to the reporting entity with our conclusion or a request for more information. If a submitted vulnerability is determined to be valid, Schneider Electric will perform an assessment of the vulnerability to determine the risk to customers; products affected, field population, and severity.

3. Mitigation

Schneider Electric determines the root cause of the issue and develops a resolution or remediation. 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 disclosure. General disclosures are published on the Schneider Electric corporate website on the second Tuesday of the month, unless the disclosure is limited to a specific group of customers in which case customers may be contacted directly to support remediation.

Each disclosure announcement contains:

- Overall description of the vulnerability including CVSS score and CVE (Schneider Electric is a CVE Numbering Authority in association with MITRE.)
- Identification of products and versions affected
- Patches or mitigating actions to reduce the risk of exploit, including patch download instructions where applicable. Schneider always encourages customers to take advantage of these updates and/or instructions and patch their installations appropriately
- With the consent of the reporting entity, Schneider Electric will identify the researcher to give credit for their discovery

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:
pub 2048R/01573082 2016-01-11 CPCERT <cybersecurity@schneider-electric.com>
https://keyserver.pgp.com/vkd/SubmitSearch.event?SearchCriteria=cybersecurity%40schneider-electric.com

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

Appendix

The following products will now be managed by the AVEVA cybersecurity team. For information on how to reach AVEVA support for your product, please refer to this link: AVEVA Software Global Customer Support for any cybersecurity needs and visit https://sw.aveva.com/support/cyber-security-updates for cybersecurity bulletins and information.

Avantis DSS MES Ampla
Avantis.Pro OASyS eDNA
CEM OGX
Citect Pipephase
ClearSCADA PRiSM
Cloud HMI PRO/II
Connoisseur Prometheus
DYNSIM QI Analyst
EBS Recipe Manager Plus
eDNA ROMeo
EMI SDO
eSCADA SimCentral
EYESIM SimSci APC
FSIM SimSuite
HEXTRAN Simulated Control Processor
8-Mar-18 Page 2 of 2
Historian SmartGlance
Historian Server Spiral
InBatch TRISIM
InduSoft Web Studio Visual Flow
InFusionSim Wonderware System
Platform InPlant Wonderware MES
Intelatrac Wonderware Mobile Reporting
Connector
InTouch Wonderware Online
InTouch OMI Wonderware Information
Server LMS

Revision Control:

Version 1 *28 January 2019*	Original Release
Version 2 *05 April 2019*	This version updates the process for reporting vulnerabilities from a form on our support portal to a pre-filled email sent to cybersecurity@se.com, includes information about AVEVA products, and specifies the frequency of our security disclosures.

Product Security Office

Digitally signed by Product Security Office
Date: 2019.04.05 19:15:08 -04'00'