Schneider Electric Security Notification

APC Smart-UPS SMT, SMC, SMX, SCL, SMTL and SRT Series

08 March 2022

Overview

Schneider Electric is aware of the vulnerabilities associated with APC Smart-UPS uninterruptable power supply devices which, if compromised, may allow for potential unauthorized access and control of the device. Upon learning of these vulnerabilities, we worked diligently to develop remediations and mitigations, and disclose in a timely, responsible manner so that our customers and end-users can better protect their people, assets, and operations.

At Schneider Electric, the safety of our customers and products is our highest priority. We develop and manufacture our products to the highest safety standards in accordance with regulatory and industry guidelines. Our UPS products are compliant to these standards, ensuring they operate in a safe manner including conducting abnormal tests where components are intentionally faulted.

Our UPS units comply with industry safety standards including UL 1778, CSA 22.2 No. 107.3 in North America and IEC 62040-1 which references to generic standards CSA-C22.2 No. 60950-1 /UL 60950-1or IEC 60950-1 / IEC 62477-1.

We recommend that customers immediately install available firmware updates provided below, which include remediations to reduce the risk of successful exploitation of these vulnerabilities. In addition, customers should also immediately ensure they have implemented cybersecurity best practices across their operations to protect themselves from exploitation of these vulnerabilities. Where appropriate, this includes locating their systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; preventing mission-critical systems and devices from being accessed from outside networks. More information on recommended security practices can be found in the General Security Recommendations section below.

Please subscribe to the Schneider Electric security notification service to be informed of updates to this notification https://www.schneider-electric.com/en/work/support/cybersecurity/security-notifications.jsp

For additional information and support, please contact your Schneider Electric sales or service representative or Schneider Electric's Customer Care Center.

Affected Products and Versions

Product	Affected Versions	CVEs
Smart-UPS Family		
SMT Series	SMT Series ID=18: UPS 09.8 and prior SMT Series ID=1040: UPS 01.2 and prior SMT Series ID=1031: UPS 03.1 and prior	**CVE-2022-0715**
SMC Series	SMC Series ID=1005: UPS 14.1 and prior SMC Series ID=1007: UPS 11.0 and prior SMC Series ID=1041: UPS 01.1 and prior	

SCL Series	SCL Series ID=1030: UPS 02.5 and prior SCL Series ID=1036: UPS 02.5 and prior	**CVE-2022-0715**
SMX Series	SMX Series ID=20: UPS 10.2 and prior SMX Series ID=23: UPS 07.0 and prior	
SRT Series	SRT Series ID=1010/1019/1025: UPS 08.3 and prior SRT Series ID=1024: UPS 01.0 and prior SRT Series ID=1020: UPS 10.4 and prior SRT Series ID=1021: UPS 12.2 and prior SRT Series ID=1001/1013: UPS 05.1 and prior SRT Series ID=1002/1014: UPSa05.2 and prior	
SmartConnect Family		
SMT Series	SMT Series ID=1015: UPS 04.5 and prior	**CVE-2022-22805** **CVE-2022-22806** **CVE-2022-0715**
SMC Series	SMC Series ID=1018: UPS 04.2 and prior	
SMTL Series	SMTL Series ID=1026: UPS 02.9 and prior	
SCL Series	SCL Series ID=1029: UPS 02.5 and prior SCL Series ID=1030: UPS 02.5 and prior SCL Series ID=1036: UPS 02.5 and prior SCL Series ID=1037: UPS 03.1 and prior	
SMX Series	SMX Series ID=1031: UPS 03.1 and prior	

Vulnerability Details

CVE ID: **CVE-2022-22805**

CVSS v3.1 Base Score 9.0 | Critical | CVSS:3.1/ AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

A *CWE-120: CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')* vulnerability exists that could cause remote code execution when an improperly handled TLS packet is reassembled.

CVE ID: **CVE-2022-22806**

CVSS v3.1 Base Score 9.0 | Critical | CVSS:3.1/ AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

A *CWE-294: Authentication Bypass by Capture*-replay vulnerability exists that could cause an unauthenticated connection to the UPS when a malformed connection is sent.

CVE ID: **CVE-2022-0715**

For Connected Devices:

CVSS v3.1 Base Score 8.9 | High | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:H/A:H

For Non-Connected Devices:

CVSS v3.1 Base Score 6.9 | Medium | CVSS:3.1/AV:P/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:H

A *CWE-287: Improper Authentication* vulnerability exists that could cause an attacker to arbitrarily change the behavior of the UPS if a key is leaked and used to upload malicious firmware.

Schneider Electric Security Notification

Remediation & Mitigations

Affected Products	Remediation
Smart-UPS SMT and SMC Series (Versions above) **SmartConnect SMT and SMC Series** (Versions above)	Firmware Version UPS 04.6 (SMT series) and Version UPS 04.3 (SMC series) include a partial remediation for **CVE-2022-0715**, which will reduce the risk of successful exploitation, for the Smart-UPS SMT and SMC series and a fix for **CVE-2022-22805** and **CVE-2022-22806** for the SmartConnect UPS SMT and SMC series. There are three ways to apply this remediation: 1. For units connected to the SmartConnect Portal, new firmware will become available automatically. Follow prompts via the portal or display to install new firmware. 2. For units not connected to the SmartConnect Portal, use the Firmware Upgrade Wizard to install the new firmware. 3. For those devices which include a NMC, it can be used to remotely update the firmware of the UPS. When downloading updates, only download from the official Schneider Electric sources above and ensure that hashes are verified before installation. *Note: After the firmware is installed, the unit will lose the capability to install future firmware via the NMC. All other methods of firmware update will continue to be available. A future firmware update will be released to re-enable this feature.* To verify new firmware version post-installation: Go to the About screen on local display, the SmartConnect portal, or on the NMC and confirm that the UPS firmware Revision is UPS 04.6 (SMT series) and UPS 04.3 (SMC series) In addition to the remediations above, customers should immediately apply the General Security Recommendations provided below to reduce the risk of exploit.
Smart-UPS SCL, SMX, and SRT Series (Versions above) **SmartConnect SMTL, SCL, and SMX Series** (Versions above)	Schneider Electric is establishing a remediation plan for Smart-UPS SCL, SMX, and SRT Series and SmartConnect SMTL, SCL, and SMX Series that will include fixes for these vulnerabilities. We will update this document when the remediation is available. Until then, customers should immediately apply the following mitigations provided below to reduce the risk of exploit: • If applicable, from the front panel disable the SmartConnect feature. • Alternately, customers may choose to disconnect any network cable connected to the UPS. • Follow the General Security Recommendations provided below

Schneider Electric Security Notification

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance applying or removing a patch.

To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here:

https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Never connect programming software to any network other than the network intended for that device.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

Acknowledgements

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher
CVE-2022-22805 CVE-2022-22806 CVE-2022-0715	Gal Levy (Armis)

Schneider Electric Security Notification

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page: https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1.0 *08 March 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.03.07 13:43:01 -08'00'