Schneider Electric Security Notification

APC Smart-UPS SMT, SMC, SMX, SCL, SRC, XU, XP, CSH2, SURTD, SMTL, SRT, and select SRTL Series

08 March 2022 (22 November 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.

November 2022 Update: SURTD series was removed from the affected products table after a further investigation concluded that it was not affected by CVE-2022-0715. SRTL series was added to the available remediation section (page 5). In addition, SMC/SMX/SMT series was added to the available remediation section (page 7) and SRC series moved to separate remediation sections (page 6).

Affected Products and Versions

Product	Affected Versions	CVEs
Smart-UPS Family		
SMT Series	SMT Series ID=14/17: UPS 14.9 and prior SMT Series ID=18: UPS 14.9 and prior SMT Series ID=1040: UPS 14.9 and prior SMT Series ID=1031: UPS 14.9 and prior SMT Series ID=1039: UPS 14.9 and prior SMT Series ID=20: UPS 14.9 and prior SMT Series ID=1041: UPS 14.9 and prior	**CVE-2022-0715**
SMC Series	SMC Series ID=1000: UPS 14.9 and prior SMC Series ID=1005: UPS 14.9 and prior SMC Series ID=1007: UPS 14.9 and prior SMC Series ID=1008: UPS 14.9 and prior	
SCL Series	SCL Series ID=1036: UPS 14.9 and prior SCL Series ID=1029: UPS 14.9 and prior SCL Series ID=1037: UPS 14.9 and prior	
SMX Series	SMX Series ID=10/11: UPS 14.9 and prior SMX Series ID=1012: UPS 14.9 and prior SMX Series ID=20: UPS 14.9 and prior SMX Series ID=23: UPS 14.9 and prior SMX Series ID=1023: UPS 14.9 and prior SMX Series ID=1003: UPS 14.9 and prior SMX Series ID=1031: UPS 14.9 and prior	
SRT Series	SRT Series ID=1010/1019/1025: UPS 14.9 and prior SRT Series ID=1020: UPS 14.9 and prior SRT Series ID=1021: UPS 14.9 and prior SRT Series ID=1001/1013: UPS 14.9 and prior SRT Series ID=1002/1014: UPS 14.9 and prior	
Only the following SRTL Series: SRTL1000RMXLI, SRTL1000RMXLI-NC SRTL1500RMXLI, SRTL1500RMXLI-NC SRTL2200RMXLI, SRTL2200RMXLI-NC SRTL3000RMXLI, SRTL3000RMXLI-NC	SRTL Series ID=1024: UPS 14.9 and prior	**CVE-2022-0715**

SRC Series	SRC Series ID=1004: UPS 13.9 and prior SRC Series ID=1006: UPS 13.9 and prior SRC Series ID=1011: UPS 13.9 and prior	**CVE-2022-0715**
XU Series	XU Series ID=1017: UPS 02.6 and prior XU Series ID=1033: UPS 00.3 and prior XU Series ID=1025: UPS 14.9 and prior	**CVE-2022-0715**
XP Series	XP Series ID=1016: UPS 02.3 and prior	**CVE-2022-0715**
CHS2 Series	CHS2 Series ID=5008: UPS 14.9 and prior	**CVE-2022-0715**
SmartConnect Family		
SMT Series	SMT Series ID=1015: UPS 04.5 and prior SMT Series ID=1031: UPS 14.9 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 14.9 and prior	
SCL Series	SCL Series ID=1030: UPS 14.9 and prior	
SMX Series	SMX Series ID=1031: UPS 14.9 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: 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.

Remediation & Mitigations

Affected Products	Remediation & Mitigation
SmartConnect SMT, SMTL, SCL, SMX Series and SMC Series (Versions above)	Firmware Version UPS 04.6 (SMT series), Version UPS 15.0 (SMTL, SCL, SMX series) and Version UPS 04.3 (SMC series) includes 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, SMTL, SCL, SMX series 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, SRT, SRTL, CSH2 & XU Series (Versions above)	Firmware Version UPS 15.0 (SRT, SRTL, CSH2, & XU series) and Firmware Version UPS 15.1 (SCL series) includes a partial remediation for CVE-2022-0715, which will reduce the risk of successful exploitation for the Smart-UPS SCL, SRTL, CSH2, XU, and SRT series. There are two ways to apply this remediation: 1. For all units, use the Firmware Upgrade Wizard to install the new firmware. 2. 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, or on the NMC and confirm that the UPS firmware Revision is UPS 15.0. In addition to the remediations above, customers should immediately apply the General Security Recommendations provided below to reduce the risk of exploit.

Smart-UPS SRC, Series (Versions above)	Firmware Version UPS 15.0 (SRC) includes a partial remediation for CVE-2022-0715, which will reduce the risk of successful exploitation for the Smart-UPS SRC series. There are two ways to apply this remediation: 1. For all units, use the Firmware Upgrade Wizard to install the new firmware. 2. 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, or on the NMC and confirm that the UPS firmware Revision is UPS 15.0. In addition to the remediations above, customers should immediately apply the General Security Recommendations provided below to reduce the risk of exploit.

Smart-UPS SMT, SMC, SMX, and XP (Versions above)	Firmware Version UPS 15.0 (SMT, SMC, SMX, XP series) includes a partial remediation for CVE-2022-0715, which will reduce the risk of successful exploitation for the Smart-UPS SMT, SMC, SMX, XP series. There are two ways to apply this remediation: 1. For all units, use the Firmware Upgrade Wizard to install the new firmware. 2. 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, or on the NMC and confirm that the UPS firmware Revision is UPS 15.0. In addition to the remediations above, customers should immediately apply the General Security Recommendations provided below to reduce the risk of exploit.

Schneider Electric Security Notification

Smart-UPS Family *SMT Series ID=14/17: UPS 14.9 and prior*	UPS models from these series with the specified IDs have been phased out and firmware remediation is not available for them. To reduce the risk of exploit, customers should continue to follow the General Security Recommendations. To remediate the vulnerabilities, we recommend that you replace UPS models with the specified IDs with a newer version of a similar model. If you have questions about which model you should procure, please reach out to your account manager or refer to the UPS Selector and Product Substitution & Replacements tools at www.apc.com.
Smart-UPS Family *SMC Series ID=1000/1008: UPS 14.9 and prior*	
Smart-UPS Family *SMX Series ID=10/11/1012: UPS 14.9 and prior*	
Smart-UPS Family *SRC Series ID=1004: UPS 14.9 and prior*	

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 these vulnerabilities:

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

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

Schneider Electric Security Notification

About Schneider Electric

Schneider's purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.

www.se.com

Revision Control:

Version 1.0 *08 March 2022*	Original Release
Version 2.0 *24 March 2022*	Added SRTL series to affected products. Removed Smart-UPS series from available remediations section as only SmartConnect currently has available remediations.
Version 3.0 *10 May 2022*	Added SRC & XU series to affected products. Added SmartConnect SMTL, SCL, and SMX Series in available remediations section.

Schneider Electric Security Notification

Version 4.0 *14 June 2022*	Added XP series to affected products. Added SRT and SCL Series in available remediations section.
Version 5.0 *12 July 2022*	SMT Series ID=1039: UPS 14.9 and prior and SMC Series ID=1041: UPS 14.9 and prior added to the Affected Products and Versions section. Added SRC, XU in the available remediations section. Various changes were made to improve clarity.
Version 6.0 *19 August 2022*	In the Affected Products and Versions section, new series IDs were added to SMT, SMC, and SMX (page 2). Added CSH2 to the available remediations sections (page 5). Added mitigations for products with the specified IDs that have been phased out and will not have firmware remediation (page 6).
Version 7.0 *22 November 2022*	SURTD series was removed from the affected products table after a further investigation concluded that it was not affected by CVE-2022-0715. SRTL series was added to the available remediation section (page 5). In addition, SMC/SMX/SMT series was added to the available remediation section (page 7) and SRC series moved to separate remediation sections (page 6).

Product Security Office

Digitally signed by Product Security Office
Date: 2022.11.21 14:04:05 -05'00'