National Computer Board

CERT-MU

CERT-MU Security Alert

Date of Issue: 10 March 2022

TLStorm Vulnerabilities: Zero-Click Flaws in Widely Used UPS Devices Threaten Critical Infrastructure

Description

Security researchers have discovered three critical security vulnerabilities dubbed as "TLStorm" in APC Smart-UPS devices, which number about 20 million in deployment worldwide. APC is a subsidiary of Schneider Electric, one of the leading vendors of UPS devices. UPS devices provide emergency backup power for mission-critical assets that require high availability. These vulnerabilities could be exploited by malicious actors to remotely take over the devices and use them to breach a company's internal network and steal data. Moreover, by cutting power for mission-critical appliances or services, attackers also could cause physical injury or disrupt business services. Moreover, an attacker can exploit the flaws to gain code execution on a device, which in turn could be used to alter the operation of the UPS to physically damage the device itself or other assets connected to it.

The latest APC Smart-UPS models are controlled through a cloud connection, and a bad actor who successfully exploits TLStorm vulnerabilities could remotely take over devices from the internet without any user interaction or the user ever knowing about it according to security researchers.

The risk for widespread disruption and damage in both the cyber and physical worlds is high if the vulnerabilities are exploited and could have an impact on a global scale. The discovery of TLStorm vulnerabilities also underscores the volatility of devices within enterprise networks that are responsible for power reliability and other critical infrastructure.

CERT-MU advises organisations with APC Smart UPS devices deployed to act immediately to protect them against security threats.

Technical Details

Two of the vulnerabilities involve the TLS connection between the UPS and the Schneider Electric cloud. Devices that support the SmartConnect feature automatically establish a TLS connection upon startup or whenever cloud connections are temporarily lost.

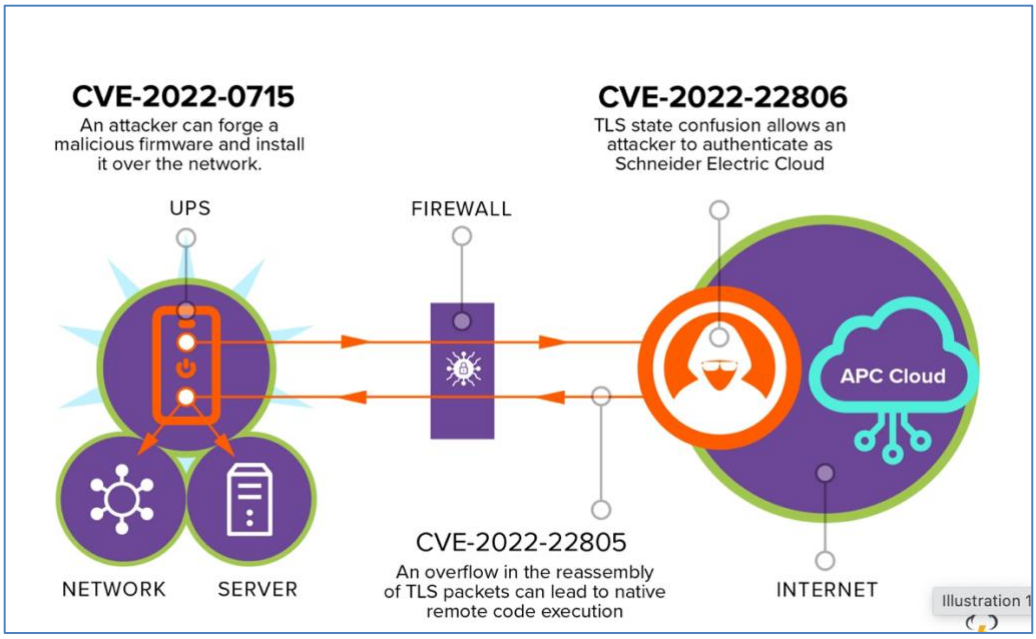
- CVE-2022-22806 – TLS authentication bypass: A state confusion in the TLS handshake leads to authentication bypass, leading to remote code execution (RCE) using a network firmware upgrade.

- CVE-2022-22805 – TLS buffer overflow: A memory corruption bug in packet reassembly (RCE).

These vulnerabilities can be triggered via unauthenticated network packets without any user interaction (ZeroClick attack).

- CVE-2022-0715 – Unsigned firmware upgrade that can be updated over the network (RCE).

The third vulnerability is a design flaw in which the firmware updates on affected devices are not cryptographically signed in a secure manner. This means an attacker could craft malicious firmware and install it using various paths, including the Internet, LAN, or a USB thumb drive. This can allow attackers to establish long-lasting persistence on such UPS devices that can be used as a stronghold within the network from which additional attacks can be carried.



Affected Systems

Smart-UPS Family

Product	Affected Versions	CVEs
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	CVE-2022-0715
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	CVE-2022-0715
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	CVE-2022-0715

SmartConnect Family

Product	Affected Versions	CVEs
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	CVE-2022-22805 CVE-2022-22806 CVE-2022-0715
SMTL Series	SMTL Series ID=1026: UPS 02.9 and prior	CVE-2022-22805 CVE-2022-22806 CVE-2022-0715
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	CVE-2022-22805 CVE-2022-22806 CVE-2022-0715
SMX Series	SMX Series ID=1031: UPS 03.1 and prior	CVE-2022-22805 CVE-2022-22806 CVE-2022-0715

Mitigations to secure your UPS

There are a few steps that you can take to minimize the risk of an attack. It is recommended using all three mitigations and not just updating the device.

1. Install the patches by Schneider Electric, which is available on:

   https://www.se.com/ww/en/product-range/61930-firmware-upgrades/

2. If you are using the NMC, change the default NMC password ("apc") and install a publicly-signed SSL certificate so that an attacker on your network will not be able to intercept the new password. To further limit the attack surface of your NMC, refer to the Schneider Electric Security Handbook for NMC 2 and NMC 3.

3. Deploy access control lists (ACLs) in which the UPS devices are only allowed to communicate with a small set of management devices and the Schneider Electric Cloud via encrypted communications.

Disclaimer

The information you have accessed or received is provided "as is" for informational purposes only. All content on this security alert is TLP: WHITE. Recipients may share TLP: WHITE information without restriction, subject to copyright controls.

Report Cyber Incidents

Let us unite together for a Safe Mauritian cyberspace during this crisis situation.

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
National Computer Board
Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu
MAUCORS: http://maucors.govmu.org