UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00253

TLSTORM VULNERABILITIES IN APC SMART UPS

DATE ISSUED: 15th March 2022

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

The popular APC Smart Uninterrupted Power Supply (UPS) devices have three new vulnerabilities associated with them, discovered by the research group Armis, that could allow an attacker to cause damage both in the cyber and physical sense.

BREAKDOWN

A UPS device is normally put in place to protect critical infrastructure from damage and loss during a power failure to keep devices running until they can be safely shut down. If exploited, these vulnerabilities could allow attackers to completely take over the devices and in some cases cause devices to ignite by overloading voltage regulation. These zero-click attacks are being tracked as CVE-2022-22806 – a TLS authentication bypass, CVE-2022-22805 – a TLS buffer overflow, both leading to Remote Code Execution (RCE) and CVE-2022-0175 – an unsigned firmware upgrade that can be updated via the network connection. The first two take advantage of the device's connection to Schneider Electric Cloud platform and the third may be exploited over various means by installing malicious firmware directly via the Internet, over a LAN, or using USB drives.

REMEDIATION STEPS

- Install patches provided on the Schneider Electric Website
- If NMC is in use, change the default NMC password and install a publicy signed SSL certificate to prevent intercept of the new password.
- Use Access Control Lists (ACLs) to restrict the number of management devices and Schneider Electric Cloud the UPS can communicate with.

REFERENCES & RESOURCES

Armis	https://www.armis.com/research/tlstorm/
Threatpost	https://threatpost.com/zero-click-flaws-ups-critical-infratructure/178810/
Scheider Electric	https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp