CYBERSECURITY POLICY AND INCIDENTS BRIEFING

INTELLIGENT BUILDINGS℠

ICYMI: Intelligent Buildings spotlights APC Smart-UPS TLStorm vulnerabilities that allow attackers to cause cyber and physical damage through undetected remote access.

03/09/22

SUMMARY

Over 20 million APC Smart-UPS (or uninterruptible power supply) devices are currently deployed worldwide. These devices are widely used in Commercial Real Estate, banking, hospitals, data centers, and media. Armis security researchers found a flaw, dubbed TLStorm, that allows attackers to take over these devices remotely. TLStorm has two critical vulnerabilities:

- One in a design flaw, in which firmware upgrades of all Smart-UPS devices are not properly signed and validated
- One in the TLS implementation used by both Cloud-connected Smart-UPS devices and a third critical vulnerability

WHAT IT MEANS

APC Smart-UPS devices are in most OT environments, server rooms, medical facilities, and even residences, and, according to Armis, 79.3% of all of these segments are vulnerable to TLStorm. This means that an attacker exploiting the TLStorm vulnerabilities could remotely take over devices without any user interaction or signs of attack. As a result, attackers can perform a remote-code execution (RCE) attack on a device, which could be used to alter the operations of the UPS to physically damage the device itself or other assets connected to it.

These attacks could have devastating consequences. Because they regulate high voltage and are Internet-connected, an attacker could use their remote access to cause an explosion. Armis was actually able to remotely ignite a Smart-UPS device. They also found that they could use the device to breach a company's network to steal data. At the very least, the attacker could cut power to mission-critical devices, disrupting business services.

You can prepare by:

- Inventorying your devices and identifying if you have APC Smart-UPS devices
- Changing all default username and passwords on your devices
- Placing these devices into security zones
- Limiting communication to and from these devices using ZeroTrust
- Installing a publicly signed SSL certificate
- Communicating only to the Schneider Electric Cloud via encrypted communications

HOW INTELLIGENT BUILDINGS CAN HELP

We have assessed thousands of buildings in the US, Canada, and overseas. In our experience, most building owners don't know what's connected, how it's connected and configured, and do not have recovery strategies in place. For example, even if backups are being performed, they are usually not being performed correctly or securely. Intelligent Buildings can **assess your building systems and the contractors** who support them to provide you with an easy-to-follow plan to secure your building control systems. Additionally, our managed service can ensure these steps are being followed and **bring your systems and contractors into compliance**.

For more information about this incident and other news, contact us at info@intelligentbuildings.com