Se han revelado tres vulnerabilidades de seguridad de alto impacto en los dispositivos Smart-UPS de APC, que podrían ser utilizados por atacantes remotos como un arma física para acceder a ellos y controlarlos de forma no autorizada.

Denominadas colectivamente como TLStorm, las vulnerabilidades *«permiten la toma remota completa de dispositivos Smart-UPS y la capacidad de llevar a cabo ataques cibernéticos extremos»*, dijeron Ben Seri y Barak Hadad, investigadores de la compañía de seguridad IoT Armis.

Los dispositivos de fuente de alimentación ininterrumpida (UPS) funcionan como proveedores de energía de respaldo de emergencia en entornos de misión crítica, como instalaciones médicas, salas de servidores y sistemas industriales. La mayoría de los dispositivos afectados, por un total de más de 20 millones, se han identificado hasta ahora en los sectores de atención médica, minorista, industrial y gubernamental.

TLStorm consiste en 3 vulnerabilidades críticas que se pueden desencadenar por medio de paquetes de red no autenticados sin requerir ninguna interacción del usuario, lo que significa que es un ataque de clic cero, con dos de los problemas relacionados con un caso de protocolo de enlace TLS defectuoso entre el UPS y la nube de APC:

- CVE-2022-22805 (puntaje CVSS: 9.0) – Desbordamiento de búfer TLS
- CVE-2022-22806 (puntaje CVSS: 9.0) – Omisión de autenticación TLS
- CVE-2022-0715 (puntaje CVSS: 8.9) – Actualización de firmware sin firmar que se puede actualizar a través de la red

La explotación exitosa de cualquiera de las vulnerabilidades podría resultar en ataques de ejecución remota de código (RCE) en dispositivos vulnerables, que a su vez podrían convertirse en armas para alterar las operaciones del UPS y dañar físicamente el dispositivo u otros activos conectados a él.

> *«Al usar nuestra vulnerabilidad RCE, pudimos eludir la protección del software y*

> *dejar que los períodos de picos de corriente se produjeran una y otra vez hasta que el capacitor del enlace de CC se calentó a ~150 grados centígrados (~300 °F), lo que provocó que el capacitor explotara y bloqueara el UPS en una nube de gas electrolito, causando daños colaterales al dispositivo»,* dijeron los investigadores.

Además, la falla en el mecanismo de actualización del firmware podría aprovecharse para plantar una actualización maliciosa en los dispositivos UPS, lo que permitiría a los atacantes establecer la persistencia durante períodos prolongados y utilizar el host comprometido como puerta de enlace para futuros ataques.

> *«El abuso de fallas en los mecanismos de actualización de firmware se está convirtiendo en una práctica estándar de las APT, como se detalló recientemente en el análisis del malware Cyclops Blink, y la firma incorrecta de firmwares de dispositivos integrados es una falla recurrente en varios sistemas integrados»*, dijeron los investigadores.

Después de la divulgación responsable a Schneider Electric el 31 de octubre de 2021, se publicaron correcciones como parte de las actualizaciones del martes de parches el 8 de marzo de 2022. Se recomienda a los clientes que instalen las actualizaciones proporcionadas para reducir el riesgo de explotar con éxito dichas vulnerabilidades.

> *«Los dispositivos UPS, como muchos otros dispositivos de infraestructura digital, por lo general se instalan y se olvidan. Debido a que estos dispositivos están conectados a las mismas redes internas que los sistemas comerciales centrales, los intentos de explotación pueden tener graves implicaciones»,* agregaron los investigadores.