Diversas vulnerabilidades de seguridad que afectan a la plataforma de Gestión de Infraestructura de Centros de Datos (DCIM) PowerPanel Enterprise de CyberPower y a la Unidad de Distribución de Energía (PDU) iBoot de Dataprobe podrían ser potencialmente aprovechadas para obtener acceso no autorizado a estos sistemas e infligir daños graves en entornos objetivo.

Las nueve vulnerabilidades, desde CVE-2023-3259 hasta CVE-2023-3267, tienen niveles de gravedad que varían de 6.7 a 9.8, permitiendo que actores de amenazas puedan apagar centros de datos completos y comprometer implementaciones de centros de datos para robar datos o lanzar ataques masivos a gran escala.

> *«Un atacante podría encadenar estas vulnerabilidades en conjunto para obtener acceso total a estos sistemas»,* informaron los investigadores de seguridad de Trellix, Sam Quinn, Jesse Chick y Philippe Laulheret.

> *«Además, ambos productos son susceptibles a la inyección remota de código que podría ser explotada para crear una puerta trasera o un punto de entrada a la red más amplia de dispositivos de centro de datos conectados y sistemas empresariales.»*

Los resultados fueron presentados hoy en la conferencia de seguridad DEFCON. No hay pruebas de que estas deficiencias hayan sido aprovechadas en la práctica. La lista de fallos, los cuales han sido abordados en la versión 2.6.9 del software PowerPanel Enterprise y en la versión 1.44.08042023 del firmware de la PDU Dataprobe iBoot, se encuentra a continuación:

PDU Dataprobe iBoot

- CVE-2023-3259 (puntuación CVSS: 9.8) – Manipulación de datos no confiables durante la deserialización, lo que conlleva a eludir la autenticación.

- CVE-2023-3260 (puntuación CVSS: 7.2) – Inserción de comandos en el sistema operativo, resultando en la ejecución remota de código autenticado.

- CVE-2023-3261 (puntuación CVSS: 7.5) – Sobrepaso del búfer, provocando una denegación de servicio (DoS).

- CVE-2023-3262 (puntuación CVSS: 6.7) – Empleo de credenciales predefinidas en el código.

- CVE-2023-3263 (puntuación CVSS: 7.5) – Elusión de la autenticación mediante un nombre alternativo.

CyberPower PowerPanel Enterprise

- CVE-2023-3264 (puntuación CVSS: 6.7) – Utilización de credenciales codificadas en el código.

- CVE-2023-3265 (puntuación CVSS: 7.2) – Neutralización inapropiada de secuencias de escape, meta o control, resultando en la elusión de la autenticación.

- CVE-2023-3266 (puntuación CVSS: 7.5) – Verificación de seguridad implementada de manera incorrecta para el estándar, provocando la elusión de la autenticación.

- CVE-2023-3267 (puntuación CVSS: 7.5) – Inserción de comandos en el sistema operativo, lo que conlleva a la ejecución remota de código autenticado.

La explotación exitosa de los defectos mencionados previamente podría afectar a despliegues de infraestructura crítica que dependen de centros de datos, resultando en apagones con un *«simple cambio»,* llevar a cabo extensos ataques de ransomware, DDoS o ataques borradores, o realizar espionaje cibernético.

> *«Una vulnerabilidad en una única plataforma de gestión de centros de datos o dispositivo puede rápidamente llevar a una compromiso total de la red interna y proporcionar a los actores de amenazas un punto de apoyo para atacar cualquier otra infraestructura conectada en la nube»*, destacaron los investigadores.