La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), publicó el martes una advertencia de aviso de sistemas de control industrial (ICS) de siete vulnerabilidades en el producto de la unidad de distribución de energía iBoot-PDU de Dataprobe, que se usa principalmente en entornos industriales y centros de datos.

> *«La explotación exitosa de estas vulnerabilidades podría conducir a la ejecución remota de código no autenticado en el dispositivo Dataprobe iBoot-PDU»,* dijo la agencia en un aviso.

A la firma de ciberseguridad industrial Claroty se le atribuye la revelación de las fallas, y dijo que las debilidades podrían activarse de forma remota *«ya sea a través de una conexión web directa al dispositivo o a través de la nube».*

iBoot-PDU es una unidad de distribución de energía (PDU) que brinda a los usuarios capacidades de monitoreo en tiempo real y mecanismos de alerta sofisticados por medio de una interfaz web para controlar el suministro de energía a los dispositivos y otros equipos en un entorno OT.

Las vulnerabilidades adquieren una nueva importancia si se tiene en cuenta el hecho de que se puede acceder a no menos de 2600 PDU en Internet, y los dispositivos Dataprobe representan casi un tercio de los expuestos, según un informe de 2021 de la plataforma de gestión de superficie de ataque Censys.

El análisis de Claroty del firmware de la PDU muestra que el producto está paralizado por problemas que van desde la inyección de comandos hasta vulnerabilidades en el recorrido de la ruta, lo que expone a los clientes a graves riesgos de seguridad.

- CVE-2022-3183 (puntuación CVSS: 9.8): Una vulnerabilidad de inyección de comandos derivada de la falta de desinfección de la entrada del usuario.
- CVE-2022-3184 (puntuación CVSS: 9.8): Una vulnerabilidad de cruce de ruta que permite el acceso a una página PHP no autenticada, que podría ser objeto de abuso

para insertar código malicioso.

La explotación remota exitosa de las vulnerabilidades *«pone a un atacante al alcance de la mano para interrumpir los servicios críticos al cortar la energía eléctrica al dispositivo, y posteriormente, cualquier cosa que esté enchufada en él»,* dijo el investigador de Claroty, Uri Katz.

Las otras cinco vulnerabilidades descubiertas (desde CVE-2022-3185 hasta CVE-2022-3189) podrían ser armadas por un mal actor para acceder a la página de administración principal del dispositivo desde la nube e incluso engañar al servidor para que se conecte a sistemas internos o externos arbitrarios (también conocido como SSRF), potencialmente filtrando información confidencial.

> *«Incluso una unidad de distribución de energía inocua administrada de forma remota por medio de Internet o a través de una plataforma de administración basada en la nube puede proporcionar un atacante predeterminado para apuntar a la red, o con una forma de interrumpir los servicios esenciales cortando la energía a los dispositivos conectados a una PDU»,* dijo Katz.

Claroty también reveló que encontró una forma de enumerar dispositivos iBoot PDU conectados a la nube mediante la explotación de una combinación de una cookie válida y la identificación del dispositivo (un valor numérico secuencial que se puede adivinar trivialmente), ampliando así la superficie de ataque disponible a todos los dispositivos conectados.

Se recomienda a los usuarios de Dataprobe iBoot-PDU que actualicen a la última versión de firmware (1.42.06162022), así como que deshabiliten SNMP, Telnet y HTTP, si no están en uso como mitigación contra algunas de estas vulnerabilidades.