La Agencia de Ciberseguridad de Infraestructura de Estados Unidos (CISA), emitió este jueves una advertencia sobre múltiples vulnerabilidades en la pila Ethernet/IP, que podría exponer a los sistemas industriales a ataques de denegación de servicio (DoS), fugas de datos y ejecución remota de código.

Todas las confirmaciones y versiones de OpENer anteriores al 10 de febrero de 2021 se ven afectadas, aunque no existen exploits públicos conocidos que se dirijan específicamente a estas vulnerabilidades.

Las cuatro vulnerabilidades de seguridad fueron descubiertas e informadas a CISA por los investigadores Tal Keren y Sharon Brizinov, de la compañía de seguridad de tecnología operativa Claroty. Además, Cisco Talos (CVE-2020-13556) reveló públicamente un quinto problema de seguridad identificado por Claroty el 2 de diciembre de 2020.

> *«Un atacante solo necesitaría enviar paquetes ENIP/CIP diseñados al dispositivo para explotar las vulnerabilidades»,* dijeron los investigadores.

CVE-2020-13556 se refiere a una vulnerabilidad de escritura fuera de los límites en el servidor Ethernet/IP, que podría permitir que un atacante envíe una serie de solicitudes de red especialmente diseñadas para desencadenar la ejecución remota de código. Tiene una calificación de 9.8 sobre 10 en gravedad.

Las otras cuatro vulnerabilidades reveladas a EIPStackGroup por los mantenedores de la pila de OpENer, en octubre de 2020, son:

- CVE-2021-27478 (puntuación CVSS de 8.2): Un error en la forma en que se manejan las solicitudes del Protocolo Industrial Común (CIP), lo que lleva a una condición DoS.
- CVE-2021-27482 (puntuación CVSS de 7.5): Un error de lectura fuera de los límites que aprovecha los paquetes especialmente diseñados para leer datos arbitrarios de la memoria.
- CVE-2021-27500 y CVE-2021-27498 (puntajes CVSS de 7.5): Dos vulnerabilidades de

afirmación alcanzables que podrían explotarse para realizar ataques DoS.

Se recomienda a los proveedores que utilicen la pila OpENer, que actualicen a la última versión, y al mismo tiempo, que tomen las medidas de protección necesarias para minimizar la exposición de la red de todos los dispositivos del sistema de control a Internet, erigir barreras de firewall y aislarlos de la red empresarial.

Esto se encuentra lejos de ser la primera vez que se descubren problemas de seguridad en las pilas EtherNet/IP. En noviembre pasado, los investigadores de Claroty revelaron una vulnerabilidad crítica descubierta en la pila 499ES EtherNet/IP de Real-Time Automation (RTA), que podría vulnerar los sistemas de control industrial a ataques remotos de hackers.