La Agencia de Seguridad Cibernética e Infraestructura de Estados Unidos (CISA) ha emitido una alerta sobre dos vulnerabilidades de seguridad que afectan a los modelos de módulos de comunicación Rockwell Automation ControlLogix EtherNet/IP (ENIP), las cuales podrían ser explotadas para lograr la ejecución remota de código y ataques de denegación de servicio (DoS).

> *«Los resultados e impacto de aprovechar estas vulnerabilidades varían según la configuración del sistema ControlLogix, pero podrían llevar a una pérdida o denegación de control, pérdida o denegación de visibilidad, robo de datos operativos o manipulación del control con consecuencias disruptivas o destructivas en el proceso industrial para el cual el sistema ControlLogix es responsable»*, afirmó Draogos.

La lista de vulnerabilidades es la siguiente:

- CVE-2023-3595 (puntuación CVSS: 9.8): Una vulnerabilidad de escritura fuera de límites que afecta a los productos 1756 EN2* y 1756 EN3*, la cual podría resultar en la ejecución de código arbitrario con persistencia en el sistema objetivo a través de mensajes maliciosamente diseñados del Protocolo Industrial Común (CIP).*
- *CVE-2023-3596 (puntuación CVSS: 7.5): Una vulnerabilidad de escritura fuera de límites que afecta a los productos 1756 EN4*, la cual podría causar una condición de denegación de servicio (DoS) a través de mensajes CIP maliciosamente diseñados.

> *«La explotación exitosa de estas vulnerabilidades podría permitir que actores maliciosos obtengan acceso remoto a la memoria en ejecución del módulo y realicen actividades maliciosas»*, indicó CISA.

Aún más preocupante, estas vulnerabilidades podrían ser utilizadas para sobrescribir cualquier parte del sistema y pasar desapercibidas, además de hacer que el módulo sea poco

confiable.

Los dispositivos afectados incluyen modelos como 1756-EN2T, 1756-EN2TK, 1756-EN2TXT, 1756-EN2TP, 1756-EN2TPK, 1756-EN2TPXT, 1756-EN2TR, 1756-EN2TRK, 1756-EN2TRXT, 1756-EN2F, 1756-EN2FK, 1756-EN3TR, 1756-EN3TRK, 1756-EN4TR, 1756-EN4TRK y 1756-EN4TRXT. Rockwell Automation ha proporcionado actualizaciones para abordar estos problemas de seguridad.

> *«El nivel de acceso que permite la vulnerabilidad CVE-2023-3595 es similar al zero-day utilizado por el grupo XENOTIME en el ataque TRISIS. Ambos permiten la manipulación arbitraria de la memoria del firmware, aunque CVE-2023-3595 se enfoca en un módulo de comunicación encargado de manejar los comandos de red. No obstante, el impacto es similar»,* mencionó la compañía de ciberseguridad industrial.

TRISIS, también conocido como TRITON, es un malware de sistemas de control industrial (ICS) que se ha detectado anteriormente atacando los controladores del sistema instrumentado de seguridad (SIS) Triconex de Schneider Electric utilizados en instalaciones de petróleo y gas. Según Dragos y Mandiant, se descubrió que una planta petroquímica en Arabia Saudita fue víctima de este ataque a finales de 2017.

Dragos advirtió que ha identificado una *«capacidad de explotación no publicada que aprovecha estas vulnerabilidades»,* asociada con un grupo estatal, y hasta mediados de julio de 2023, *«no se ha encontrado evidencia de que se estén explotando en entornos reales, y se desconoce cuáles son las organizaciones objetivo y las industrias afectadas».*

> *«Además de comprometer el módulo vulnerable en sí, esta vulnerabilidad también podría permitir que un atacante afecte el proceso industrial y la infraestructura crítica subyacente, lo que podría dar lugar a interrupciones o destrucción»,* comentó Satnam Narang, investigador de Tenable, sobre la vulnerabilidad CVE-2023-3595.