Se han revelado vulnerabilidades críticas en seis sistemas distintos de Medición Automática de Tanques (ATG) de cinco fabricantes, lo que podría exponerlos a ataques remotos.

> *«Estas fallas de seguridad representan riesgos graves en el mundo real, ya que podrían ser explotadas por actores malintencionados para generar daños a gran escala, incluidos daños físicos, riesgos ambientales y pérdidas económicas,»* explicó Pedro Umbelino, investigador de Bitsight, en un informe publicado la semana pasada.

El problema se agrava porque el análisis reveló que miles de estos ATGs están accesibles desde Internet, lo que los convierte en un objetivo atractivo para cibercriminales interesados en llevar a cabo ataques disruptivos y destructivos contra estaciones de servicio, hospitales, aeropuertos, bases militares y otras instalaciones de infraestructura crítica.

Los ATGs son sistemas de sensores que controlan los niveles de un tanque de almacenamiento (como un tanque de combustible) con el propósito de detectar fugas y monitorear parámetros. La explotación de fallos en estos sistemas puede causar consecuencias serias, como denegaciones de servicio (DoS) y daños físicos.

Las 11 vulnerabilidades recién descubiertas afectan a seis modelos de ATG: Maglink LX, Maglink LX4, OPW SiteSentinel, Proteus OEL8000, Alisonic Sibylla y Franklin TS-550. De estas fallas, ocho tienen una calificación de severidad crítica:

- CVE-2024-45066 (CVSS: 10.0) – Inyección de comandos del sistema operativo en Maglink LX.
- CVE-2024-43693 (CVSS: 10.0) – Inyección de comandos del sistema operativo en Maglink LX.
- CVE-2024-43423 (CVSS: 9.8) – Credenciales codificadas en Maglink LX4.
- CVE-2024-8310 (CVSS: 9.8) – Omisión de autenticación en OPW SiteSentinel.
- CVE-2024-6981 (CVSS: 9.8) – Omisión de autenticación en Proteus OEL8000.
- CVE-2024-43692 (CVSS: 9.8) – Omisión de autenticación en Maglink LX.

- CVE-2024-8630 (CVSS: 9.4) – Inyección SQL en Alisonic Sibylla.
- CVE-2023-41256 (CVSS: 9.1) – Omisión de autenticación en Maglink LX (duplicado de una falla anterior).
- CVE-2024-41725 (CVSS: 8.8) – Vulnerabilidad de cross-site scripting (XSS) en Maglink LX.
- CVE-2024-45373 (CVSS: 8.8) – Escalamiento de privilegios en Maglink LX4.
- CVE-2024-8497 (CVSS: 7.5) – Lectura arbitraria de archivos en Franklin TS-550.

> *«Estas vulnerabilidades permiten obtener privilegios de administrador completos sobre la aplicación del dispositivo, y algunas incluso permiten acceso total al sistema operativo. El ataque más grave consiste en manipular los dispositivos para que operen de manera que puedan causar daños físicos a sus componentes o a los equipos conectados»,* indicó Umbelino.

Vulnerabilidades encontradas en OpenPLC, Riello NetMan 204 y AJCloud

Se han identificado también fallas de seguridad en la plataforma de código abierto OpenPLC, incluyendo una vulnerabilidad crítica de desbordamiento de búfer basado en la pila (CVE-2024-34026, CVSS: 9.0), que podría ser aprovechada para ejecutar código de manera remota.

> *«Mediante el envío de una solicitud ENIP con un código de comando no compatible, un encabezado de encapsulación válido y al menos 500 bytes, es posible sobrescribir el búfer log_msg y corromper la pila. Dependiendo de las medidas de seguridad implementadas en el sistema afectado, es posible que haya una mayor explotación»,* explicó Cisco Talos.

Otra serie de fallas se ha encontrado en la tarjeta de comunicaciones de red Riello NetMan 204, utilizada en sus sistemas de alimentación ininterrumpida (UPS), lo que podría permitir a un atacante tomar el control del UPS o incluso manipular los datos registrados.

- CVE-2024-8877 – Inyección SQL en tres puntos de la API (/cgi-bin/db_datalog_w.cgi, /cgi-bin/db_eventlog_w.cgi y /cgi-bin/db_multimetr_w.cgi), permitiendo la modificación de datos arbitrarios.
- CVE-2024-8878 – Restablecimiento de contraseña sin autenticación mediante el punto /recoverpassword.html, lo que permite al atacante obtener el identificador del dispositivo (netmanid) y calcular el código de recuperación para restablecer la contraseña.

> *«Ingresar el código de recuperación en '/recoverpassword.html' restablece las credenciales de inicio a admin:admin,»* explicó Thomas Weber de CyberDanube, quien advirtió que esto podría permitir que un atacante secuestre el dispositivo y lo apague.

Ambas fallas no han sido corregidas aún, por lo que se recomienda limitar el acceso a estos dispositivos en entornos críticos hasta que se libere un parche.

También se han identificado vulnerabilidades graves en la plataforma de gestión de cámaras IP AJCloud, las cuales, de ser explotadas con éxito, podrían exponer datos sensibles de los usuarios y otorgar control remoto total sobre las cámaras conectadas al servicio de hogar inteligente.

> *«Un comando P2P preconfigurado permite acceso de escritura arbitrario a un archivo clave de configuración, lo que puede usarse para desactivar permanentemente las cámaras o facilitar la ejecución remota de código mediante la activación de un desbordamiento de búfer,»* explicó Elastic Security Labs. Hasta la fecha, los intentos por contactar a la empresa china han sido infructuosos.

CISA advierte sobre ataques continuos a redes OT

Estos desarrollos coinciden con una advertencia de la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU. (CISA) sobre el aumento de amenazas dirigidas a dispositivos de tecnología operativa (OT) y sistemas de control industrial (ICS) accesibles por Internet, incluidos los del sector de Sistemas de Agua y Aguas Residuales (WWS).

> *«Sistemas OT/ICS expuestos y vulnerables pueden permitir a actores maliciosos utilizar credenciales por defecto, realizar ataques de fuerza bruta u otros métodos rudimentarios para acceder a estos dispositivos y causar daños,»* indicó CISA.

En febrero pasado, el gobierno de los Estados Unidos impuso sanciones a seis funcionarios vinculados con la agencia de inteligencia de Irán por llevar a cabo ataques contra entidades de infraestructura crítica en EE. UU. y otros países.

Estos ataques consistieron en la explotación de controladores lógicos programables (PLCs) de la serie Unitronics Vision, fabricados en Israel, que estaban expuestos en internet utilizando contraseñas predeterminadas.

La empresa de ciberseguridad industrial Claroty ha puesto a disposición del público dos herramientas de código abierto llamadas PCOM2TCP y PCOMClient, que permiten a los usuarios recuperar información forense de los PLC/HMI integrados de Unitronics.

> *«PCOM2TCP permite convertir mensajes seriales PCOM en mensajes TCP PCOM, y viceversa. La segunda herramienta, llamada PCOMClient, permite a los usuarios conectarse a los PLC de las series Vision/Samba de Unitronics, realizar consultas y extraer datos forenses de los PLC»*, explicó Claroty.

Además, Claroty ha advertido que el uso excesivo de soluciones de acceso remoto en los

entornos de tecnología operativa (OT) —que oscila entre cuatro y 16 herramientas— genera nuevos riesgos operativos y de seguridad para las empresas.

> *«El 55% de las organizaciones implementaron cuatro o más herramientas de acceso remoto que conectan los sistemas OT con el exterior, lo cual es preocupante, ya que estas empresas tienen superficies de ataque más amplias, difíciles y costosas de gestionar»*, señaló.
>
> *«Los ingenieros y gestores de activos deben buscar activamente reducir o eliminar el uso de herramientas de acceso remoto poco seguras en los entornos OT, especialmente aquellas con vulnerabilidades conocidas o que carecen de características de seguridad esenciales, como la autenticación multifactor (MFA)».*