La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), publicó varios avisos de Sistemas de Control Industrial (ICS) que advierten sobre fallas de seguridad críticas que afectan a los productos de Sewio, InHand Networks, Sauter Controls y Siemens.

La más grave de las vulnerabilidades se relaciona con RTLS Studio de Sewio, que podría ser aprovechada por un atacante para *«obtener acceso no autorizado al servidor, alterar información, crear una condición de denegación de servicio, obtener privilegios escalados y ejecutar código arbitrario»*, según CISA.

Esto incluye CVE-2022-45444 (puntaje CVSS: 10.0), un caso de contraseñas codificadas para usuarios seleccionados en la base de datos de la aplicación que potencialmente otorgan acceso ilimitado a adversarios remotos.

También son notables dos vulnerabilidades de inyección de comandos (CVE-2022-47911 y CVE-2022-43483, puntaje CVSS: 9.1) y una vulnerabilidad de escritura fuera de los límites (CVE-2022-41989, puntaje CVSS: 9.1) que podría resultar en condición de denegación de servicio o ejecución de código.

Las vulnerabilidades afectan a RTLS Studio versión 2.0.0 hasta la versión 2.6.2 incluso. Se recomienda a los usuarios que actualicen a la versión 3.0.0 o posterior.

CISA, en una segunda alerta, destacó un conjunto de cinco vulnerabilidades en InHand Networks InRouter 302 e InRouter 615, incluyendo CVE-2023-22600 (puntuación CVSS: 10.0), que podrían provocar la inyección de comandos, la divulgación de información y la ejecución de código.

> *«Si se encadenan correctamente, estas vulnerabilidades podrían resultar en que un usuario remoto no autorizado comprometa por completo todos los dispositivos InHand Networks administrados en la nube accesibles por la nube»,* dijo la agencia.

Todas las versiones de firmware de InRouter 302 anteriores a IR302 V3.5.56 e InRouter 615 anteriores a InRouter6XX-S-V2.3.0r5542 son susceptibles a errores.

También se revelaron vulnerabilidades de seguridad en Sauter Controls Nova 220, Nova 230, Nova 106 y moduNet300 que podrían permitir la visibilidad no autorizada de información confidencial (CVE-2023-0053, puntuación CVSS: 7.5), y la ejecución remota de código (CVE-2023-0052, puntuación CVSS: 9.8).

Sin embargo, la empresa de automatización con sede en Suiza no planea lanzar soluciones para los problemas identificados debido a que la línea de productos ya no es compatible.

Finalmente, la agencia de seguridad detalló una vulnerabilidad de comandos entre sitios (XSS) en el equipo Siemens Mendix SAML (CVE-2022-46823, puntaje CVSS: 9.3) que podría permitir que un atacante obtenga información confidencial al engañar a los usuarios para que hagan clic en un enlace con código especialmente diseñado.

Se recomienda a los usuarios habilitar la autenticación multifactor y actualizar Mendix SAML a las versiones 2.3.4 (Mendix 8), 3.3.8 (Mendix 9, Upgrade Track) o 3.3.9 (Mendix 9, New Track) para mitigar los riesgos potenciales.