Se han revelado nueve vulnerabilidades de seguridad en los productos de gestión de energía eléctrica fabricados por Schweitzer Engineering Laboratories (SEL).

> *«La vulnerabilidad más crítica de esas nueve permitiría a un atacante facilitar la ejecución de código remoto (RCE) en una estación de trabajo de ingeniería», Nozomi Networks señaló en un informe publicado la semana pasada*

Estos problemas, identificados como CVE-2023-34392 y desde CVE-2023-31168 hasta CVE-2023-31175, tienen calificaciones de gravedad en el sistema de puntuación CVSS que oscilan entre 4.8 y 8.8 y afectan a los productos SEL-5030 acSELeratorQuickSet y SEL-5037 GridConfigurator, los cuales se utilizan para configurar, comisionar y supervisar estos dispositivos.

La explotación de CVE-2023-31171 podría lograrse mediante el envío de un correo electrónico de suplantación de identidad que engañe a un ingeniero objetivo para que importe un archivo de configuración especialmente diseñado, lo que permitiría la ejecución de código arbitrario en la estación de trabajo de ingeniería que esté ejecutando el software de SEL.

Además, esta vulnerabilidad podría combinarse con CVE-2023-31175 para obtener privilegios de administrador en la estación de trabajo objetivo. Por otro lado, CVE-2023-34392 podría ser utilizada por un adversario para enviar comandos arbitrarios a las máquinas de manera sigilosa mediante un ataque de *«watering hole».*

Estos últimos hallazgos de investigación se suman a un conjunto previamente reportado de 19 vulnerabilidades de seguridad en el conjunto de software de Controlador de Automatización en Tiempo Real (RTAC) de SEL (desde CVE-2023-31148 hasta CVE-2023-31166) que podrían ser explotadas para *«obtener acceso no autorizado a la interfaz web, alterar la información mostrada, manipular su lógica, llevar a cabo ataques de intermediario (MitM) o ejecutar código arbitrario».*

En julio de 2023, la empresa de seguridad de tecnología operativa también destacó cinco nuevas vulnerabilidades que afectan a la solución de software American Megatrends (AMI) MegaRAC BMC, lo que podría permitir a un atacante lograr persistencia resistente a reinicios y ocultar una puerta trasera en la interfaz de gestión BMC basada en web.

> *«Este acceso de puerta trasera podría persistir incluso después de reinstalaciones del sistema operativo principal o reinicios duros de la configuración BMC en sí misma»,* Nozomi Networks informó.

Desde entonces, se han descubierto 14 vulnerabilidades adicionales en el Phoenix Contact Web Panel 6121-WXPS, incluyendo cuatro defectos críticos, que podrían ser aprovechados por un atacante remoto para comprometer por completo los dispositivos.

Esto ocurre al mismo tiempo que la Agencia de Seguridad Cibernética e Infraestructura de Estados Unidos (CISA) ha colaborado con MITRE para desarrollar una extensión destinada a la plataforma de emulación de ataques cibernéticos Caldera, la cual se enfoca específicamente en las redes de tecnología operativa (OT).