



Investigadores descubren importantes vulnerabilidades de seguridad en las bibliotecas de protocolos MMS industriales

Han salido a la luz varios detalles sobre vulnerabilidades de seguridad en dos implementaciones del protocolo Manufacturing Message Specification (MMS) que, si son explotadas con éxito, podrían tener serios efectos en entornos industriales.

«Estas vulnerabilidades podrían permitir a un atacante desestabilizar un dispositivo industrial o, en algunos casos, ejecutar código de forma remota», señalaron los investigadores de Claroty, Mashav Sapir y Vera Mens, en un nuevo informe.

El protocolo MMS es una [especificación de mensajería](#) en la capa de aplicación del modelo OSI, que posibilita el control y la supervisión remota de dispositivos industriales mediante el intercambio de información de control de manera independiente a la aplicación específica.

Concretamente, facilita la comunicación entre dispositivos electrónicos inteligentes (IEDs) y sistemas de control y adquisición de datos (SCADA), o bien, controladores lógicos programables (PLCs).

Las cinco vulnerabilidades descubiertas por la compañía de seguridad en tecnología operativa afectan a la biblioteca [libIEC61850](#) de MZ Automation y a la biblioteca [TMW IEC 61850](#) de Triangle MicroWorks. Estas fallas fueron corregidas en septiembre y octubre de 2022 tras la divulgación responsable:

- [CVE-2022-2970](#) (Puntuación CVSS: 10.0) – Vulnerabilidad de desbordamiento de búfer en la pila de libIEC61850 que podría causar un bloqueo o ejecución remota de código.
- [CVE-2022-2971](#) (Puntuación CVSS: 8.6) – Vulnerabilidad de confusión de tipos en libIEC61850 que podría permitir a un atacante provocar la caída del servidor con una carga útil maliciosa.
- [CVE-2022-2972](#) (Puntuación CVSS: 10.0) – Vulnerabilidad de desbordamiento de búfer en la pila de libIEC61850 que también podría ocasionar un bloqueo o la ejecución remota de código.
- [CVE-2022-2973](#) (Puntuación CVSS: 8.6) – Vulnerabilidad de desreferencia de puntero nulo que podría permitir a un atacante hacer que el servidor se bloquee.



Investigadores descubren importantes vulnerabilidades de seguridad en las bibliotecas de protocolos MMS industriales

- [CVE-2022-38138](#) (Puntuación CVSS: 7.5) – Vulnerabilidad de acceso a un puntero no inicializado que podría ser utilizada por un atacante para generar una condición de denegación de servicio (DoS).

El análisis de Claroty también encontró que el dispositivo [IED SIPROTEC 5](#) de Siemens dependía de una versión antigua de la pila MMS-EASE de SISCO, lo que lo hacía vulnerable a una condición de DoS mediante un paquete especialmente diseñado ([CVE-2015-6574](#), Puntuación CVSS: 7.5).

La empresa alemana lanzó una actualización de firmware en diciembre de 2022 que incluyó una versión más reciente del protocolo, según un [aviso](#) publicado por la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA).

La investigación de Claroty [subraya](#) la «brecha entre las exigencias de seguridad de las tecnologías modernas y los protocolos obsoletos y difíciles de reemplazar», instando a los proveedores a seguir las recomendaciones de seguridad de CISA.

Esta divulgación llega pocas semanas después de que Nozomi Networks revelara dos vulnerabilidades en la implementación de referencia del protocolo inalámbrico ESP-NOW de Espressif (CVE-2024-42483 y CVE-2024-42484), que podrían permitir ataques de repetición y causar una condición de DoS.

«Dependiendo del sistema atacado, esta vulnerabilidad [CVE-2024-42483] podría tener consecuencias significativas. ESP-NOW se usa en sistemas de seguridad como alarmas de edificios, permitiendo que se comuniquen con los sensores de movimiento», explicaron.

«En un escenario así, un atacante podría explotar la vulnerabilidad para repetir un comando legítimo de 'APAGADO' previamente interceptado, desactivando un sensor de movimiento a voluntad».



Investigadores descubren importantes vulnerabilidades de seguridad en las bibliotecas de protocolos MMS industriales

De forma similar, el uso de ESP-NOW en dispositivos de apertura remota, como puertas automáticas o garajes, podría ser aprovechado para interceptar un comando de 'ABRIR' y repetirlo más tarde para acceder de forma no autorizada a un edificio.

En agosto, Nozomi Networks también informó sobre 37 vulnerabilidades no corregidas en la biblioteca de análisis libfluid_msg de OpenFlow, denominadas en conjunto como «FluidFaults», que un atacante podría explotar para bloquear aplicaciones de redes definidas por software (SDN).

«Un atacante con visibilidad de red hacia un controlador o reenviador OpenFlow puede enviar un paquete malicioso de red OpenFlow que provoque un ataque de denegación de servicio (DoS)», [advirtieron](#).

En los últimos meses, también se han descubierto vulnerabilidades en el sistema operativo TwinCAT/BSD de Beckhoff Automation, que podrían exponer los PLCs a alteraciones lógicas, ataques de denegación de servicio y hasta la ejecución de comandos con privilegios de root en el controlador.