La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) publicó esta semana una advertencia de aviso de Sistemas de Control Industrial (ICS) sobre múltiples vulnerabilidades en el software de ingeniería Mitsubishi Electic GX Works3.

> *«La explotación exitosa de estas vulnerabilidades podría permitir a los usuarios no autorizados obtener acceso a los módulos de CPU de la serie MELSEC iQ-R/F/L y al módulo de servidor OPC UA de la serie MELSEC iQ-R o ver y ejecutar programas»,* dijo la agencia.

GX Works3 es un software de estación de trabajo de ingeniería utilizado en entornos ICS, que actúa como un mecanismo para cargar y descargar programas desde/hacia el controlador, solucionar problemas de software y hardware y realizar operaciones de mantenimiento.

La amplia gama de funciones también hace posible que la plataforma sea un objetivo atractivo para los atacantes que buscan comprometer dichos sistemas para apoderarse de los PLC administrados.

Tres de las diez vulnerabilidades se relacionan con el almacenamiento de datos confidenciales en texto claro, cuatro se relacionan con el uso de una clave criptográfica codificada, dos se relacionan con el uso de una contraseña codificada y una se refiere a un caso de credenciales insuficientemente protegidas.

Los errores más críticos, CVE-2022-25164 y CVE-2022-29830, tienen una puntuación CVSS de 9.1 y se puede abusar de ellos para obtener acceso al módulo de la CPU y obtener información sobre los archivos del proyecto sin necesidad de permisos.

Nozomi Networks, que descubrió CVE-2022-29831 (puntaje CVSS: 7.5), dijo que un atacante con acceso a un archivo de proyecto de PLC de seguridad podría explotar la contraseña codificada para acceder directamente al módulo de CPU de seguridad y potencialmente interrumpir los procesos industriales.

> *«El software de ingeniería representa un componente crítico en la cadena de seguridad de los controladores industriales. Si surge alguna vulnerabilidad en ellos, los adversarios pueden abusar de ellos para comprometer en última instancia los dispositivos administrador y, en consecuencia, el proceso industrial supervisado»*, dijo la compañía.

La divulgación se produce cuando CISA reveló detalles de una vulnerabilidad de denegación de servicio (DoS) en Mitsubishi Electric MELSEC iQ-R Series, que se deriva de la falta de validación de entrada adecuada (CVE-2022-40265, puntuación CVSS: 8.6).

> *«La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto no autenticado provoque una condición de denegación de servicio en un producto de destino mediante el envío de paquetes especialmente diseñados»*, dijo CISA.

En un desarrollo relacionado, la agencia de seguridad cibernética describió además tres problemas que afectan el controlador compacto remoto (RCC) 972 de Horner Automation, el más crítico de los cuales (CVE-2022-2641, puntaje CVSS: 9.8) podría conducir a la ejecución remota de código o causar una condición DoS.