VULNERABILIDADES EN SCHNEIDER ELECTRIC'S MODICON M221 PLC

BCSC_ALERTA_VULNERABILIDADES_ SCHNEIDER_ELECTRIC_ MODICON_M221

TLP:WHITE

www.basquecybersecurity.eus

Noviembre 2020

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

RESUMEN EJECUTIVO

La gama de **controladores lógicos programables** (PLC) **Modicon M221 de Schneider Electric**, ampliamente utilizada en la automatización de las máquinas del sector industrial, cuenta con una serie de vulnerabilidades que podrían ser explotadas por un atacante no autenticado con acceso a la red OT para **romper el cifrado** empleado en el tráfico de datos entre el dispositivo M221 y el software EcoStruxure Machine Expert Basic, así como eludir la autenticación y llevar a cabo la ejecución de comandos para hacerse con el **control total** del dispositivo vulnerable.

Por su parte, Schneider Electric ha publicado una serie de **recomendaciones** y **medidas de mitigación** con el objetivo de reducir la exposición a posibles ataques, ya que, por el momento, no se prevé el lanzamiento de actualizaciones de seguridad que solucionen los fallos.

ANÁLISIS TÉCNICO

Investigadores de seguridad han reportado la existencia de cuatro vulnerabilidades en la gama de controladores lógicos programables (**PLC**) **Modicon M221** de **Schneider Electric**, dispositivos de alto rendimiento ampliamente utilizados en el sector industrial para controlar la automatización de las máquinas de forma intuitiva y flexible mejorando la eficiencia.

Las vulnerabilidades podrían permitir a un usuario no autorizado realizar modificaciones en los dispositivos vulnerables mediante una serie de ataques que consisten en la evasión de la autenticación, la rotura del cifrado empleado en la transferencia de datos y la ejecución de comandos, lo que le permitiría hacerse con el control total de los controladores.

No obstante, para realizar las modificaciones anteriormente descritas, un atacante tendría que contar previamente con presencia en la infraestructura de red OT y capturar el tráfico entre el software EcoStruxure Machine Expert Basic y los dispositivos PLC de Modicon M221, ya que la explotación de las vulnerabilidades está basada principalmente en el uso de una implementación del algoritmo de cifrado XOR débil.

A continuación, se describen las vulnerabilidades identificadas:

- **CVE-2020-7565**. La vulnerabilidad está ocasionada por la implementación de la llave de cifrado XOR de 4 bytes utilizada para cifrar los datos, ya que resulta insuficientemente robusta, lo que podría permitir a un atacante romper la clave de cifrado de escritura y lectura y capturar el tráfico entre el software de EcoStruxure Machine y el controlador Modicon. Para ello, un atacante tendría que emplear ataques de texto plano conocido, es decir, comparar secciones de memoria conocidas con sus homólogos ya cifrados, o realizar un análisis estadístico de las secuencias repetitivas de claves XOR en el tráfico.
- **CVE-2020-7566**. Los dispositivos Modicon M221 emplean una implementación criptográfica de intercambio de archivos débil, que consiste en utilizar el método de intercambio de claves Diffie-Hellman para generar una clave XOR de 4 bytes, lo que permitiría a un atacante deducir la clave empleada para la transferencia de datos mediante un ataque de fuerza bruta.
- **CVE-2020-7567**. Las comunicaciones entre el software de EcoStruxure Machine y los controladores Modicon están protegidas mediante el cifrado XOR de 4 bytes, por lo que un atacante que lograse deducir la clave de cifrado, mediante cualquiera de los métodos anteriormente expuestos, podría utilizar esta clave para averiguar el hash de la contraseña de transferencia de datos y usar un tipo de ataque de movimiento lateral denominado *Pass-the-Hash* para autenticarse en el dispositivo.

- **CVE-2020-7568**. Algunas secciones de memoria son accesibles sin que sea requerida contraseña alguna, incluso si las protecciones de lectura y escritura se encuentran activadas, lo que permitiría a un atacante acceder a información restringida.

Por el momento, la base de datos del **NIST** no ha registrado ninguna de estas vulnerabilidades, si bien, en el aviso publicado por Schneider Electric, este ha otorgado a las vulnerabilidades una puntuación de **7.1** según la escala **CVSSv3**.

Hasta la fecha, no se tiene conocimiento de la explotación activa de estas vulnerabilidades en la red, ni la disponibilidad de exploits o pruebas de concepto públicamente disponibles que aprovechen los fallos.

Schneider Electric ha confirmado que **todas las versiones** de la gama de controladores lógicos programables (PLC) **Modicon M221** se ven afectadas por estas vulnerabilidades.

MITIGACIÓN / SOLUCIÓN

En el aviso de seguridad publicado por Schneider Electric, en ausencia de actualizaciones que solucionen los fallos, este ha incluido una serie de **medidas de mitigación** a aplicar con el objetivo de reducir el riesgo de exposición a posibles ataques. Las medidas de mitigación descritas por el fabricante se detallan a continuación:

- Establecer una **segmentación de la red** e implementar un **firewall** con el propósito de bloquear todos los accesos no autorizados al **puerto** TCP **502**.
- **Deshabilitar** todos los **protocolos no utilizados**, especialmente el protocolo de **programación**, para evitar el acceso involuntario a la funcionalidad de programación de forma remota.

  Para llevar a cabo esta medida, se recomienda consultar la sección "Configuración de la red de Ethernet" de la guía EcoStruxure Machine Expert - Ayuda básica online para PLC M221.
- Establecer una contraseña segura para:
  - Proteger la infraestructura.
  - Restringir el acceso de lectura en el dispositivo.
  - Restringir el acceso de escritura en el dispositivo.

  Es importante establecer contraseñas diferentes para cada uno de los propósitos anteriormente descritos.

De manera adicional, la compañía ha ofrecido una lista con una serie de **buenas prácticas** en ciberseguridad aplicadas al ámbito industrial:

- Proteger las redes de los sistemas de control y seguridad industrial mediante firewall y aislarlas del resto de la red empresarial.
- Impedir que personal no autorizado acceda a los sistemas de control y seguridad industrial.
- No conectar el software de programación a ninguna red que no sea la específica para ello.
- Escanear todos los métodos de intercambio de datos con la red aislada antes de utilizarlos en los terminales o en cualquier nodo conectado a las redes de los sistemas de control y seguridad industrial.
- Reducir la exposición de las redes de los sistemas de control y seguridad industrial asegurando que no sean accesibles desde Internet.
- Utilizar métodos de acceso remoto seguro, tales como VPN.

REFERENCIAS ADICIONALES

- Schneider Electric Security Notification - Modicon M221 Programmable Logic Controller
- Claroty, Schneider Electric disclose Modicon M221 authentication bypass flaws

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?