Boletín de octubre de 2019

Avisos de Sistemas de Control Industrial

Desbordamiento de búfer en routers de la serie EDR-810 de Moxa

Fecha de publicación: 02/10/2019

Importancia: Alta

Recursos afectados:

Routers de la serie EDR-810, versiones de *firmware* 5.1 y anteriores.

Descripción:

Moxa ha reportado una vulnerabilidad, de tipo desbordamiento de búfer basado en pila (*stack*), que afecta a los routers de la serie EDR-810. La explotación exitosa de esta vulnerabilidad permitiría a un atacante ejecutar código arbitrario.

Solución:

Moxa ha publicado una actualización de *firmware* que soluciona esta vulnerabilidad.

Detalle:

Existen múltiples funciones en el servidor web que podrían permitir a un atacante provocar un desbordamiento de búfer, dando lugar a la ejecución de código arbitrario.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Siemens

Fecha de publicación: 08/10/2019

Importancia: Alta

Recursos afectados:

- CP1616 y CP1604: todas las versiones anteriores a 2.8;
- Kits de desarrollo o evaluación para PROFINET IO:
  - DK Standard Ethernet Controller: todas las versiones;
  - EK-ERTEC 200: todas las versiones;
  - EK-ERTEC 200P: todas las versiones.
- SIMATIC CFU PA: todas las versiones anteriores a 1.2.0;
- SCALANCE X-200IRT: todas las versiones anteriores a 5.2.1;
- SIMATIC ET 200AL, 200M, 200S, 200pro: todas las versiones;
- SIMATIC ET 200MP IM 155-5 PN BA: todas las versiones anteriores a 4.2.3;
- SIMATIC ET 200MP IM 155-5 PN HF y ST: todas las versiones;
- SIMATIC ET 200SP IM 155-6 PN BA, HA, HS y ST: todas las versiones;
- SIMATIC ET 200SP IM 155-6 PN HF y PN/2 HF: todas las versiones anteriores a 4.2.2;
- SIMATIC ET 200SP IM 155-6 PN/3 HF: todas las versiones anteriores a 4.2.1;
- SIMATIC ET 200ecoPN (excepto 6ES7148-6JD00- 0AB0 y 6ES7146-6FF00-0AB0): todas las versiones;
- SIMATIC IT UADM: todas las versiones anteriores a 1.3;
- SIMATIC HMI Comfort Outdoor Panels 7" & 15": todas las versiones;
- SIMATIC HMI Comfort Panels 4" - 22": todas las versiones;
- SIMATIC HMI KTP Mobile Panels: todas las versiones;
- SIMATIC PN/PN Coupler: todas las versiones;

- SIMATIC PROFINET Driver: todas las versiones anteriores a 2.1;
- SIMATIC S7-1200 familia CPU (incl. F): todas las versiones;
- SIMATIC S7-1500 familia CPU (incl. F): todas las versiones anteriores a 2.0;
- SIMATIC S7-300 familia CPU (incl. F): todas las versiones;
- SIMATIC S7-400 (incl. F) V6 y anteriores: todas las versiones;
- SIMATIC S7-400 PN/DP V7 (incl. F): todas las versiones;
- SIMATIC S7-400H V6: todas las versiones anteriores a 6.0.9;
- SIMATIC S7-410 V8: todas las versiones;
- SIMATIC WinAC RTX (F) 2010: todas las versiones;
- SIMOTION: todas las versiones;
- SINAMICS DCM: todas las versiones anteriores a 1.5 HF1;
- SINAMICS DCP: todas las versiones;
- SINAMICS G110M V4.7 (Control Unit): todas las versiones anteriores a la V4.7 SP10 HF5;
- SINAMICS G120 V4.7 (Control Unit): todas las versiones anteriores a la V4.7 SP10 HF5;
- SINAMICS G130 V4.7 (Control Unit): todas las versiones;
- SINAMICS G150 (Control Unit): todas las versiones;
- SINAMICS GH150 V4.7 (Control Unit): todas las versiones;
- SINAMICS GL150 V4.7 (Control Unit): todas las versiones;
- SINAMICS GM150 V4.7 (Control Unit): todas las versiones;
- SINAMICS S110 (Control Unit): todas las versiones;
- SINAMICS S120 V4.7 (Control Unit and CBE20): todas las versiones;
- SINAMICS S150 (Control Unit): todas las versiones;
- SINAMICS SL150 V4.7 (Control Unit): todas las versiones;
- SINAMICS SM120 V4.7 (Control Unit): todas las versiones;
- SINUMERIK 828D: todas las versiones anteriores a la V4.8 SP5;
- SINUMERIK 840D sl: todas las versiones.

Descripción:

Se han publicado múltiples vulnerabilidades del tipo denegación de servicio y credenciales insuficientemente protegidas. La explotación de estas vulnerabilidades podría permitir a un atacante causar una pérdida de sincronización en tiempo real de los dispositivos y efectuar un ataque de denegación de servicio en los mismos, así como obtener la contraseña para poder acceder a la estación TeamCenter conectada a la instancia del sistema.

Solución:

Consultar la sección de *Referencias*.

Detalle:

- Un atacante no autenticado con acceso a la red del producto afectado podría causar una condición de denegación de servicio mediante la ruptura de la sincronización en tiempo real (IRT) de la instalación afectada. No es necesaria interacción del usuario para la explotación de dicha vulnerabilidad. Se ha reservado el identificador CVE-2019-10923 para esta vulnerabilidad.
- Los dispositivos afectados contienen una vulnerabilidad que permite a un atacante no autenticado causar una denegación de servicio. Dicha vulnerabilidad puede ser explotada si una gran cantidad de paquetes UDP, especialmente diseñados, son enviados al dispositivo. La explotación exitosa de esta vulnerabilidad no requiere ni privilegios de sistema, ni interacción del usuario. Se ha reservado el identificador CVE-2019-10936 para esta vulnerabilidad.
- Las versiones afectadas del software SIMATIC WinAC RTX (F) 2010 contienen una vulnerabilidad que podría permitir a un atacante no autenticado causar una condición de denegación de servicio. Dicha vulnerabilidad puede ser explotada si una gran cantidad de peticiones HTTP son enviadas al servicio en ejecución. La explotación exitosa de esta vulnerabilidad no requiere ni privilegios de sistema, ni interacción del usuario. Se ha reservado el identificador CVE-2019-13921 para esta vulnerabilidad.
- Un atacante remoto autenticado con acceso al puerto 1434/tcp del producto SIMATIC IT UADM podría conseguir la contraseña con la que obtener accesos de lectura y escritura a la estación TeamCenter. Esto se debe a que las contraseñas son cifradas con una clave de encriptación predecible. No se requiere de una interacción del usuario. Se ha reservado el identificador CVE-2019-13929 para esta vulnerabilidad.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en productos de Schneider Electric

Fecha de publicación: 09/10/2019

Importancia: Alta

Recursos afectados:

- Modicon M580 (todas las versiones de firmware),
- Modicon M340 (todas las versiones de firmware),
- Modicon Premium (todas las versiones de firmware),
- Modicon Quantum (todas las versiones de firmware),
- Modicon BMxCRA and 140CRA modules (todas las versiones de firmware),
- Modicon Premium (todas las versiones de firmware),
- Modicon Quantum (todas las versiones de firmware),
- Modicon BMENOC 0311,
- Modicon BMENOC 0321.

Descripción:

Se han publicado múltiples vulnerabilidades del tipo exposición de información de archivo y directorio, excepciones no controladas en el programa, transmisión en claro de información sensible y exposición de la misma, que podrían permitir a un atacante obtener información sensible o provocar una denegación de servicio.

Solución:

El fabricante no ha liberado parches para estas vulnerabilidades, en su lugar detalla pasos a seguir para mitigar el problema en función del producto afectado. Consultar la sección de referencias para más información.

Detalle:

A continuación, se detallan las vulnerabilidades de severidad alta:

- La vulnerabilidad del tipo exposición de información de archivo y directorio, podría permitir a un atacante obtener información del controlador cuando el protocolo TFTP está en uso. Se ha asignado el identificador CVE-2019-6851 para esta vulnerabilidad.
- La vulnerabilidad del tipo exposición de información podría permitir a un atacante obtener información sensible cuando están en uso servicios de Modbus provistos por el REST API del módulo de comunicación del controlador. Se han asignado los identificadores CVE-2019-6849 y CVE-2019-6850 para esta vulnerabilidad.
- La vulnerabilidad del tipo excepción no controlada en el programa, podría permitir a un atacante causar una denegación de servicio en el PLC al mandar datos específicos al API REST del módulo de comunicación del controlador. Se ha asignado el identificador CVE-2019-6848 para esta vulnerabilidad.

Para el resto de las vulnerabilidades, se han asignado los identificadores: CVE-2019-6841, CVE-2019-6842, CVE-2019-6843, CVE-2019-6844, CVE-2019-6845, CVE-2019-6846 y CVE-2019-6847.

Etiquetas: Schneider Electric, Vulnerabilidad

Vulnerabilidad CSRF en Sunny WebBox de SMA Solar Technology AG

Fecha de publicación: 09/10/2019

Importancia: Crítica

Recursos afectados:

Sunny WebBox, versión 1.6 de *firmware* y anteriores.

Descripción:

Los investigadores Borja Merino y Eduardo Villaverde, de la Universidad de León, junto con Carlos del Canto y Victor Fidalgo, del área de ciberseguridad para Sistemas de Control Industrial de INCIBE, han reportado una vulnerabilidad, de tipo CSRF (*Cross-Site Request Forgery*), que permitiría a un atacante remoto realizar acciones con los permisos del usuario.

Solución:

El producto actual no tiene soporte, por lo que SMA recomienda aplicar las siguientes medidas:

- Desactivar la redirección de puertos y emplear una VPN.
- Cambiar todas las contraseñas por defecto.
- Cerrar todos los puertos del sistema o router que no vayan a usarse.

Detalle:

La explotación de esta vulnerabilidad por parte de un atacante podría generar una condición de denegación de servicio, la modificación de contraseñas, activar servicios, realizar ataques *man-in-the-middle* y modificar los parámetros de entrada de los dispositivos, como por ejemplo sensores. El atacante envía un enlace malicioso a un operador autenticado, lo que permitiría a este ejecutar acciones con los permisos de dicho usuario. Se ha reservado el identificador CVE-2019-13529 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en el controlador Mark Vle de GE

Fecha de publicación: 09/10/2019

Importancia: Media

Recursos afectados:

Todas las versiones del controlador Mark Vle.

Descripción:

El investigador Sharon Brizinov de Claroty ha reportado varias vulnerabilidades en el software que afecta al controlador Mark Vle. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante la lectura, escritura o ejecución comandos en el controlador.

Solución:

GE recomienda las siguientes soluciones para mitigar estos problemas:

- Deshabilitar el servicio Telnet, que se encuentra habilitado por defecto en el controlador Mark Vle en las versiones 6.0 y anteriores.
- Cambiar la contraseña al desplegar el controlador Mark Vle dentro del entorno operativo.

Detalle:

- Una vulnerabilidad se debe a una implementación insegura del protocolo Telnet en el dispositivo. Un atacante podría autenticarse con credenciales predeterminadas. Se ha reservado el identificador CVE-2019-13554 para esta vulnerabilidad.
- La otra vulnerabilidad se debe a la existencia de credenciales embebidas, con privilegios de *root,* en el dispositivo. Un atacante podría acceder controlador con privilegios de *root*.

Etiquetas: Actualización, Vulnerabilidad

Denegación de servicio en TwinCAT Profinet driver de Beckhoff Automation

Fecha de publicación: 10/10/2019

Importancia: Alta

Recursos afectados:

Todas las versiones guales o inferiores de:

- TwinCAT 2 Build 2304,
- TwinCAT 3.1 Build 4024.0.

Descripción:

El investigador Andreas Galauner de Rapid7 ha reportado una vulnerabilidad de criticidad alta que afecta a múltiples dispositivos. Un atacante remoto podría generar una condición de denegación de servicio en los dispositivos.

Solución:

Actualmente no hay actualizaciones que solucionen la vulnerabilidad, Bechoff está trabajando en ellas. Mientras tanto, recomiendan aplicar reglas en el firewall para bloquear paquetes PROFINET DCP procedentes de redes no confiables al dispositivo.

Detalle:

TwinCAT incluye un controlador Profinet que podría ser configurado en un entorno de desarrollo para enviar conexiones Profinet al controlador. En el caso de que esto se haya configurado, se podrían enviar paquetes Profinet DCP manipulados. Un atacante remoto podría enviar estos paquetes manipulados para generar una condición de denegación de servicio en el dispositivo. Se ha reservado el identificador CVE-2019-5637 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en productos Infinity M300 de Dräger

Fecha de publicación: 11/10/2019

Importancia: Alta

Recursos afectados:

Infinity® M300 VG2.3.1 y anteriores.

Descripción:

DrÃ¤ger ha descubierto múltiples vulnerabilidades de tipo denegación de servicio y exposición de información que podría permitir a un atacante remoto causar una denegación de servicio en el dispositivo y obtener información transmitida a través de la red del hospital.

Solución:

DrÃ¤ger liberará en marzo del 2020 una actualización de software, la VG2.3.2.

Detalle:

- En el caso de que un atacante no autorizado ejecute un ataque de denegación de servicio en la red del hospital, la red Infinity podría comprometerse y suponer un reinicio de los productos Infinity M300 o una pérdida de su comunicación inalámbrica. Un reinicio lleva unos 30 segundos, tiempo durante el cual habrá una pérdida de monitorización del paciente, sin embargo, se reanudará de forma automática. La Infinity CentralStation alertará sonora y visualmente cuando el Infinity M300 está desconectado.
- Un ataque de denegación de servicio reiterado podría hacer que el Infinity M300 entre en un estado de error, requiriendo un reinicio manual.
- En el caso de que un atacante no autorizado consiga acceder a la red del hospital y atacar la red Infinity, la información enviada entre el Infinity CentralStation y el Infinity M300 se vería comprometida, permitiéndole cambiar ajustes de las alarmas, apagarlas o poner el M300 en estado de suspensión o descarga.

Etiquetas: Vulnerabilidad

Vulnerabilidad de desbordamiento de búfer en el driver IEC870IP de AVEVA

Fecha de publicación: 15/10/2019

Importancia: Alta

Recursos afectados:

Driver IEC870IP para Vijeo Citect y Citect SCADA, versión 4.14.02 y anteriores.

Descripción:

El equipo VAPT, del centro IIT Kanpur, en colaboración con el ICS-CERT, ha descubierto una vulnerabilidad, de tipo desbordamiento de

búfer de memoria, que podría permitir a un atacante provocar una caída del servidor y dejarlo fuera de funcionamiento.

Solución:

Se recomienda actualizar los productos afectados a la versión 4.15.00.

Detalle:

Las versiones vulnerables del driver IEC870IP se ven afectadas por un desbordamiento de búfer. En el caso de que un atacante explote dicha vulnerabilidad, podría provocar que el servidor dejase de funcionar correctamente.

Etiquetas: Actualización, SCADA, Vulnerabilidad

Múltiples vulnerabilidades en Automation Worx Software Suite de Phoenix Contact

Fecha de publicación: 15/10/2019

Importancia: Alta

Recursos afectados:

- PC Worx, versión 1.86 y anteriores.
- PC Worx Express, versión 1.86 y anteriores.
- Config , versión 1.86 y anteriores.

Descripción:

El equipo de 9sg Security Team, coordinado por NCCIC y , ha reportado múltiples vulnerabilidades, de tipo lectura fuera de límites y corrupción de memoria, debido a una ejecución de código remoto causada por una validación incorrecta de los datos de entrada.

Solución:

En la siguiente versión del producto se implementarán mejoras para corregir estos problemas, hasta la fecha se recomienda aplicar una serie de medidas para mitigar dichas vulnerabilidades:

- Al compartir ficheros de proyectos, utilizar servicios seguros para la transferencia.
- No compartir información sensible a través de correos sin encriptación.

Detalle:

Las modificaciones en proyectos de PC Works o Config permitirían a un atacante la ejecución de código remoto, debido a una validación incorrecta de los datos de entrada. El atacante necesita tener acceso al dispositivo con proyectos de Worx o Config para poder modificar los datos y ficheros del proyecto. El atacante cambia los ficheros originales por los modificados, causando así el ataque. Se ha reservado el identificador CVE-2019-16675 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en múltiples productos de Eaton.

Fecha de publicación: 18/10/2019

Importancia: Alta

Recursos afectados:

- CGLine Web Controller, versión Z1000.H y anteriores,
- CGVision, versiones desde la 6.02 hasta la 6.40.

Descripción:

Eaton ha reportado una vulnerabilidad que afecta a CGLine Web Controller cuando se conecta al software de supervisión CGVision.

Solución:

- CGLine Web Controller, actualizar a la versión Z1000.J. Para poder descargar la nueva versión del firmware, han de ponerse en contacto con el servicio de atención de Eaton.
- CGVision, está prevista una actualización para noviembre de 2019.

Detalle:

A la hora de conectar el software de supervisión CGVision al dispositivo CGLine Web Controller, se genera una vulnerabilidad que afecta a ambos dispositivos. Los dispositivos CGLine Web Controller, que no están conectados o supervisados por el CGVision, no se ven afectados por dicha vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Cscape de Horner Automation

Fecha de publicación: 18/10/2019

Importancia: Alta

Recursos afectados:

Cscape, versión 9.90 y anteriores.

Descripción:

El investigador Francis Provencher, de Protek Research Lab, junto con Zero Day Initiative de Trend Micro, han reportado vulnerabilidades de tipo escritura fuera de límites y validación de entradas inadecuada, las cuales permitirían el acceso a información y ejecución de código de forma arbitraria.

Solución:

Horner Automation recomienda a los usuarios afectados actualizar a la versión 9.90 SP1 o superior de Cscape, disponibles para Estados Unidos o el resto del mundo.

Detalle:

- Una incorrecta validación en el procesamiento de archivos podría permitir a un atacante crear archivos especialmente diseñados, lo que permitiría el acceso a información confidencial o la ejecución remota de código arbitrario. Se ha reservado el identificador CVE-2019-13541 para esta vulnerabilidad.
- Una validación incorrecta de los datos puede hacer que el sistema escriba fuera de la zona de búfer prevista, lo que puede permitir la ejecución arbitraria del código por parte de un atacante. Se ha reservado el identificador CVE-2019-13545 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Autenticación incorrecta en múltiples dispositivos de ABB

Fecha de publicación: 18/10/2019

Importancia: Baja

Recursos afectados:

- UNO-DM, versión 1.8.2 y anteriores;
- PVS-100-TL y PVS120-TL, versión 0.10.14 y anteriores;
- PVS-175-TL, versión 0.2.6 y anteriores;
- PVS-50/60 y TRIO-TM, versión 1.2.15 y anteriores;
- REACT 2, versión 0.2.19 y anteriores.

Descripción:

El investigador Maxim Rupp ha reportado una vulnerabilidad de autenticación incorrecta que podría permitir a un atacante tener acceso a la información de los productos afectados sin necesidad de autenticarse.

Solución:

Actualizar a las siguientes versiones:

- UNO-DM versión 1.8.3.
- PVS-100-TL y PVS120-TL versión 0.10.15.
- PVS-175-TL versión 0.2.7.
- PVS-50/60 y TRIO-TM versión 1.2.16.
- REACT 2 versión 0.2.20.

Detalle:

La vulnerabilidad de tipo autenticación incorrecta podría permitir que el producto tuviera acceso a cierta información en modo lectura sin la necesidad de realizar un proceso de autenticación previo. No se ha asignado identificador para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de desbordamiento de búfer en CODESYS ENI de 3S-Smart Software Solutions GmbH

Fecha de publicación: 24/10/2019

Importancia: Crítica

Recursos afectados:

- Servidores CODESYS V2.3 ENI, versiones anteriores a 3.2.2.25.
- Configuraciones CODESYS V2.3, versiones anteriores a 2.3.9.61, ya que contienen versiones vulnerables del servidor CODESYS ENI afectado.

Descripción:

Se ha identificado una vulnerabilidad, de tipo desbordamiento de búfer, que afecta a los servidores ENI de 3S-Smart Software Solutions

GmbH. Un atacante podría provocar una condición de denegación de servicio o ejecutar código arbitrario de manera remota.

Solución:

El fabricante recomienda actualizar el producto afectado a la versión 3.2.2.25 para solucionar esta vulnerabilidad.

Detalle:

Un atacante remoto podría explotar esta vulnerabilidad, de tipo desbordamiento de búfer basado en la pila (*stack*), para provocar una condición de denegación de servicio o realizar una ejecución de código arbitrario. Se ha reservado el identificador CVE-2019-16265 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Falta de autenticación en IP-AK2 de Honeywell

Fecha de publicación: 25/10/2019

Importancia: Media

Recursos afectados:

- Panel de control de acceso IP-AK2 versión 1.04.07 y anteriores.

Descripción:

El investigador Maxim Rupp ha reportado una vulnerabilidad de tipo falta de autenticación en función crítica que podría permitir a un atacante descargar ficheros de configuración a través de URL sin autentificación, revelando configuración e información de visitantes autorizados.

Solución:

Actualizar a la versión 1.04.15.

Detalle:

El servidor web integrado de los dispositivos afectados podría permitir a atacantes remotos, sin autenticación, obtener datos de configuración de la web. Se ha asignado el identificador CVE-2019-13525 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Chiller SK 3232-Series de Rittal

Fecha de publicación: 25/10/2019

Importancia: Crítica

Recursos afectados:

Interfaz web de Chiller SK 3232-Series basada en el *firmware* Carel pCOWeb A1.5.3 ? B1.2.4.

Descripción:

Applied Risk ha reportado varias vulnerabilidades, de tipo falta de autenticación en función crítica y uso de credenciales embebidas, en el producto Chiller SK 3232-Series de Rittal. La explotación exitosa de estas vulnerabilidades podría interrumpir las operaciones primarias del componente afectado, apagar el enfriamiento de otros equipos y permitir cambios en el punto de ajuste de temperatura.

Solución:

Para obtener información sobre las mitigaciones de estas vulnerabilidades se recomienda contactar con el soporte de Rittal a través de la siguiente dirección de correo: .

Detalle:

- El mecanismo de autenticación en los sistemas afectados no proporciona un nivel suficiente de protección contra cambios de configuración no autorizados. Las operaciones primarias, es decir, el encendido y apagado de la unidad de refrigeración y el ajuste del punto de ajuste de la temperatura, pueden modificarse sin necesidad de autenticación. Se ha reservado el identificador CVE-2019-13549 para esta vulnerabilidad.
- El mecanismo de autenticación en los sistemas afectados se configura utilizando credenciales embebidas. Estas credenciales podrían permitir a los atacantes influir en las operaciones primarias de los sistemas afectados, a saber, encender y apagar la unidad de refrigeración y establecer el punto de ajuste de temperatura. Se ha reservado el identificador CVE-2019-13553 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Exposición de recursos en IntelliSpace Perinatal de Philips

Fecha de publicación: 25/10/2019

Importancia: Media

Recursos afectados:

IntelliSpace Perinatal versión K y anteriores.

Descripción:

Philips ha identificado una vulnerabilidad de criticidad media. Un atacante podría conseguir acceso sin autorización a los recursos del sistema, incluyendo la ejecución de software o ver/modificar ficheros, directorios, o la configuración del sistema.

Solución:

Philips actualizará la documentación disponible en el portal Philips InCenter para proporcionar una guía clara sobre las mitigaciones.

Detalle:

La vulnerabilidad dentro del entorno de la aplicación IntelliSpace Perinatal podría permitir que un atacante no autorizado con acceso físico a una pantalla de aplicación bloqueada, o a un usuario de la aplicación de sesión de escritorio remoto autorizado, puedan acceder a recursos no autorizados del sistema operativo Windows, como usuario de Windows con acceso limitado. Debido a las posibles vulnerabilidades de Windows, es posible que se utilicen métodos de ataque adicionales para escalar los privilegios en el sistema operativo. Se ha reservado el identificador CVE-2019-13546 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de ABB

Fecha de publicación: 28/10/2019

Importancia: Crítica

Recursos afectados:

- Relion 650 series, versión 2.1.0.2 y anteriores;
- Relion 670 series, versión 2.1.0.2 y anteriores;
- Relion 670 series, versión 1p1r26 y anteriores.

Descripción:

Se han publicado múltiples vulnerabilidades del tipo denegación de servicio, exposición de información y acceso no autorizado a archivos que podrían permitir a un atacante obtener información sensible o causar la denegación de servicio.

Solución:

Actualizar los productos afectados a la ultima versión. Para más información consultar la sección de referencias.

Detalle:

Un atacante que aprovechara alguna de las vulnerabilidades descritas en este aviso, podría llegar a realizar alguna de las siguientes acciones:

- denegación de servicio,
- divulgación de información,
- recuperar cualquier archivo de la unidad flash.

Se han asignado los identificadores: CVE-2016-2109, CVE-2016-2177, CVE-2016-2178, CVE-2016-2182, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306, CVE-2017-3737, CVE-2018-0739, CVE-2018-0737 y CVE-2018-0732.

Etiquetas: Actualización, Vulnerabilidad

Acceso no autorizado a redes adyacentes en productos FL NAT de Phoenix Contact

Fecha de publicación: 28/10/2019

Importancia: Alta

Recursos afectados:

- FL NAT 2208;
- FL NAT 2304-2GC-2SFP.

Descripción:

Phoenix Contact ha descubierto una vulnerabilidad de criticidad alta en dispositivos FL NAT. Un atacante podría obtener acceso no autorizado a subredes adyacentes al dispositivo.

Solución:

Phoenix Contact publicará una actualización de firmware (V2.90) en el Q2 de 2020 solucionando dicha vulnerabilidad.

Detalle:

La vulnerabilidad es posible si las seguridades basadas en puerto MAC o 802.1x se encuentran activadas. Los dispositivos afectados podrían permitir el acceso no autorizado a subredes adyacentes, en el caso de que se haga una transmisión enrutada. Un atacante podría obtener acceso no autorizado a subredes adyacentes al dispositivo. Se ha reservado el identificador CVE-2019-18352 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad