Boletín de febrero de 2019

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en PremiSys de IDenticard

Fecha de publicación: 01/02/2019

Importancia: Crítica

Recursos afectados:

- PremiSys todas las versiones anteriores a 4.1

Descripción:

El investigador Jimi Sebree, trabajando con Tenable, ha reportado varias vulnerabilidades del tipo administración inadecuada de credenciales, encriptación poco robusta y contraseña inadecuada, que podrían permitir a un potencial atacante ver información confidencial u obtener acceso a los dispositivos y al sistema como administrador.

Solución:

- IDenticard ha publicado la versión 4.1 de su software que soluciona alguna de las vulnerabilidades. En febrero de 2019 lanzarán una actualización para las otras vulnerabilidades. Además, IDenticard sugiere cambiar usuario y contraseña predeterminado de la base de datos de servicio.

Detalle:

- Un atacante podría conseguir las credenciales de administrador. Se ha asignado el CVE-2019-3906 a esta vulnerabilidad.
- El sistema almacena las credenciales y otra información de interés con una encriptación débil, lo cual podría permitir a un atacante tener acceso a la información. Se ha asignado el CVE-2019-3907 a esta vulnerabilidad.
- El sistema almacena las copias de seguridad como archivos zip cifrados mediante una contraseña idéntica y que no se puede cambiar. Esto podría permitir a un atacante acceso a la información si consigue la contraseña. Se ha asignado el CVE-2019-3908 a esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en los switches EDS-405A, EDS-408A, EDS-510A y IKS-G6824A de Moxa

Fecha de publicación: 01/02/2019

Importancia: Crítica

Recursos afectados:

- Switches de las series EDS-405A, EDS-408A y EDS-510A versión 3.8 o anteriores.
- Switches de la serie IKS-G6824A versión 4.5 o anteriores.

Descripción:

Moxa a notificado varias vulnerabilidades de tipo almacenamiento de contraseña en texto plano, desbordamiento de búfer, XSS, acceso de control inadecuado, CSRF, lecturas de memoria, gestión de paquetes OSPF, identificador predecible, consumo de recursos y falta de cifrado que afectan a sus Switches de las series EDS-405A, EDS-408A, EDS-510A y IKS-G6824A. Un potencial atacante podría ejecutar código remoto, recuperar contraseñas, conseguir una denegación de servicio, resetear el dispositivo, leer posiciones de memoria o modificar configuraciones.

Solución:

- Moxa ha publicado un parche que soluciona estas vulnerabilidades. Además, recomienda habilitar la configuración web a modo solo https para las series EDS-405A, EDS-408 y EDS-510A, y deshabilitar la consola web para la serie IKS-G6824A.

Detalle:

- **Almacenamiento en texto plano**: Un potencial atacante autenticado podría ejecutar código arbitrario desde la consola.
- **Identificador predecible**: Un potencial atacante podría recuperar la contraseña de administrador aprovechándose de que el valor de la cookie de sesión no es generado con el cifrado correcto.
- **Falta de cifrado**: Un potencial atacante podría aprovechar la falta de cifrado en los protocolos propietarios utilizados por los switches para recuperar la contraseña de administrador.
- **Restricción inadecuada de intentos de autenticación**: Un potencial atacante podría utilizar fuerza bruta para recuperar contraseñas, ya que no existe un control de intentos de autenticación fallidos.
- **Consumo de recursos**: Un potencial atacante remoto podría enviar paquetes especialmente manipulados de los protocolos propietarios y conseguir una denegación de servicio.
- **Desbordamiento de búfer**: Los switches disponen de varios desbordamientos de búfer que podrían ser aprovechados por un potencial atacante para ejecutar código remoto o reiniciar el dispositivo.
- **Lecturas de memoria**: Un potencial atacante podría leer direcciones arbitrarias de memoria, ya que no se comprueban adecuadamente los límites de los arrays.
- **Gestión de paquetes OSPF**: Un potencial atacante podría enviar paquetes «Hello OSPF» malformados y conseguir el reinicio del dispositivo.
- **XSS**: Un potencial atacante puede aprovechar fallos en la validación de las entradas para realizar ataques de tipo XSS.
- **Acceso de control inadecuado**: Un potencial atacante con permisos de solo lectura podría llegar a modificar la configuración debido a que la autorización no se comprueba adecuadamente.
- **CSRF**: Un potencial atacante podría usar el navegador de un usuario autenticado para causar un ataque de tipo CSRF.

No se ha asignado CVE para ninguna de las vulnerabilidades.

Etiquetas: Comunicaciones, Vulnerabilidad

Ejecución remota de código en InduSoft Web Studio e InTouch Edge HMI de AVEVA

Fecha de publicación: 04/02/2019

Importancia: Crítica

Recursos afectados:

- InduSoft Web Studio, versiones anteriores a la 8.1 SP3
- InTouch Edge HMI (Touch Machine Edition), versiones anteriores a 2017 Update 3

Descripción:

Tenable ha identificado dos vulnerabilidades de tipo falta de autenticación para función crítica y control inadecuado de identificación de recursos que afectan al software InduSoft Web Studio e InTouch Edge HMI de AVEVA. Un atacante remoto no autenticado podría ejecutar procesos arbitrarios usando ficheros de configuración de conexiones de base de datos especialmente modificados.

Solución:

AVEVA ha publicado nuevas versiones de software que solucionan estas vulnerabilidades.

- InduSoft Web Studio, versión 8.1 SP3
- InTouch Edge HMI (Touch Machine Edition), versión 2017 Update 3

Detalle:

- Un atacante no autenticado podría usar ficheros de configuración de conexiones de base de datos especialmente modificados para ejecutar procesos en Server Machine con los permisos de software InduSoft Web Studio e InTouch Edge HMI y comprometer el servidor.

Etiquetas: SCADA, Vulnerabilidad

Gestión inadecuada de paquetes en Ethernet/IP Web Server Module de Rockwell Automation

Fecha de publicación: 05/02/2019

Importancia: Media

Recursos afectados:

- Ethernet/IP Web Server Module 1756-EWEB (incluidos 1756-EWEBK), versión v5.001 y anteriores.
- Ethernet/IP Web Server Module de controladores CompactLogix 1768-EWEB, versión v2.005 y anteriores.

Descripción:

Tenable ha identificado una vulnerabilidad de tipo gestión inadecuada de paquetes en Ethernet/IP Web Server Module de Rockwell Automation que podría permitir a un atacante remoto provocar una denegación de comunicaciones mediante SNMP hasta que el dispositivo se reinicie.

Solución:

Rockwell Automation no ha publicado una mitigación en forma de parche o actualización para esta vulnerabilidad y aconseja a todos los usuarios deshabilitar el servicio SNMP siguiendo el manual del producto, siempre y cuando no lo utilicen.

También recomienda realizar las siguientes acciones:

- Utilizar controles en la infraestructura de red, como pueden ser cortafuegos, para controlar el tráfico SNMP.
- Bloquear todo el tráfico Ethernet/IP y de cualquier otro protocolo basado en CIP desde fuera de la zona de fabricación, controlando el puerto 161/UDP.
- Usar software con garantías.
- Minimizar la exposición de la red.
- Ubicar los dispositivos y redes de control detrás de cortafuegos.
- Usar VPN si el acceso externo es requerido.

Detalle:

- Un atacante no autenticado podría enviar paquetes UDP malformados que afecten al servicio SNMP del dispositivo. La gestión inadecuada de estos paquetes podría resultar en una denegación de servicio para SNMP (puerto 161/UDP) hasta que el dispositivo se reinicie. La interfaz web seguirá indicando que el servicio está en ejecución, aunque no sea así. Se ha reservado el identificador CVE-2018-19016 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en pasarelas Modbus PR100088 de Kunbus

Fecha de publicación: 06/02/2019

Importancia: Crítica

Recursos afectados:

- Modbus PR100088 Gateway, todas las versiones anteriores a la *release* R02 o versión de software 1.1.13166

Descripción:

Nicolas Merle, de Applied Risk, ha identificado varias vulnerabilidades de tipo autenticación inadecuada, falta de autenticación en funciones críticas y validación de entradas inadecuada. Un atacante podría lograr una condición denegación de servicio o ejecutar código arbitrario.

Solución:

- Kunbus recomienda actualizar a la versión R02.

Detalle:

- Un atacante podría cambiar la contraseña del usuario *admin* si éste se ha logeado previamente en el sistema. Se ha reservado el identificador CVE-2019-6527 para esta vulnerabilidad.
- Un atacante no autenticado podría leer y escribir valores en los registros de almacenamiento de usuario. Se ha reservado el identificador CVE-2019-6533 para esta vulnerabilidad.
- Un atacante podría enviar una petición FTP maliciosa y causar un fallo en el dispositivo. Se ha reservado el identificador CVE-2019-6529 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en dispositivos Siemens

Fecha de publicación: 12/02/2019

Importancia: Crítica

Recursos afectados:

- Las variantes de firmware MODBUS TCP, DNP3 TCP, IEC104, Profinet IO para el módulo Ethernet EN100, todas las versiones.
- La variante de firmware IEC 61850 para el módulo Ethernet EN100, versiones anteriores a 4.35
- Relays SIPROTEC 5 con módulo de comunicación Ethernet EN100:
  - CPU CP300 y CP100, versiones anteriores a 7.82
  - CPU CP200, versiones anteriores a 7.58
- SIMATIC FieldPG M5, versiones anteriores a 22.01.06
- SIMATIC IPC427E, IPC477E versiones anteriores a 21.01.09
- SIMATIC IPC547E, versiones anteriores a R1.30.0
- SIMATIC IPC547G, versiones anteriores a R1.23.0
- SIMATIC IPC627D, IPC677D, IPC827D versiones anteriores a 19.02.11
- SIMATIC IPC647D, IPC847D versiones anteriores a 19.01.14
- SIMATIC ITP1000, versiones anteriores a 23.01.04
- SIMATIC ITC1500 V3 y V3 PRO, ITC1900 V3 y V3 PRO, ITC2200 V3 y V3 PRO, versiones anteriores a 3.1
- SICAM 230, versión 7.20 y anteriores.

Descripción:

El investigador Lars Lengersdorf de Amprion GmbH ha reportado la vulnerabilidad del tipo de denegación de servicio, las demás han sido detectadas y gestionadas por Siemens.

Solución:

- SIMATIC FieldPG/IPC/ITP descargar la actualización a través del siguiente enlace:
  - FieldPG M5 actualizar a la versión 22.01.06
  - IPC427E, IPC477E actualizar a la versión 21.01.09
  - IPC547E actualizar a la versión R1.30.0
  - IPC547G actualizar a la versión R1.23.0
  - IPC627D, IPC677D y IPC827D actualizar a la versión 19.02.11

    - IPC647D y IPC847D actualizar a la versión 19.01.14
    - ITP1000 actualizar a la versión 23.01.04
- Firmware IEC 61850 para Ethernet EN100actualizar a la versión 4.35
- Para Firmware MODBUS, DNP3 TCP, IEC104 y Profinet IO para Ethernet EN100 bloquear el acceso al puerto 102/tcp mediante un cortafuegos externo.
- SIPROTEC 5:
    - CPU CP300 y CP100, actualizar a la versión 7.82
    - CPU CP200, actualizar a la versión 7.58
- SIMATIC ITC1500 V3 y V3 PRO, ITC1900 V3 y V3 PRO, ITC2200 V3 y V3 PRO, actualizar a la versión 3.1
- SICAM 230 con versiones anteriores a 7.20 actualizar o aplicar WibuKey Digital Rights Management (DRM) con versión 6.5 o superior desde WIBU SYSTEMS.

Detalle:

Un usuario malintencionado que aprovechara alguna de las vulnerabilidades descritas, podría llegar a realizar las siguientes acciones en los productos afectados:

- Denegación de servicio.
- Escalada de privilegios.
- Ejecución de código.
- Revelar información sensible.

Se han asignado los identificadores CVE-2018-3616, CVE-2018-3657, CVE-2018-3658, CVE-2017-5753, CVE-2018-3639, CVE-2018-3989, CVE-2018-3990 y CVE-2018-3991 y reservado el identificador CVE-2018-16563 para estas vulnerabilidades.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Cross-site scripting en PI visión de OSIsoft

Fecha de publicación: 13/02/2019

Importancia: Baja

Recursos afectados:

- PI Vision 2017
- PI Vision 2017 R2

Descripción:

OSIsoft ha identificado una vulnerabilidad de tipo cross-site scripting (XSS) que afecta a sus dispositivos PI Vision. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante leer y modificar el contenido de la página web de PI Vision y los datos relacionados con la aplicación de PI Vision en el navegador de la víctima.

Solución:

- OSIsoft recomienda a los usuarios actualizar PI Vision a la versión 2017 R2 SP1

Detalle:

- La aplicación contiene una vulnerabilidad de cross-site scripting donde se muestran referencias a elementos AF y atributos que contienen JavaScript. Esta vulnerabilidad requiere para su explotación que un usuario AF autorizado almacene JavaScript en los elementos y atributos de AF. Se ha asignado el identificador CVE-2018-19006 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en PowerMonitor 1000 de Rockwell Automation

Fecha de publicación: 14/02/2019

Importancia: Crítica

Recursos afectados:

- Monitores PowerMonitor 1000, todas las versiones.

Descripción:

Rockwell Automation ha identificados dos vulnerabilidades del tipo *cross-site scripting* (*XSS*) y evasión de autenticación en sus monitores PowerMonitor 1000 que podrían permitir a un atacante remoto sin autenticación la inyección de código en el navegador web del usuario, el uso de funcionalidades restringidas a usuarios administradores o la modificación de la configuración del usuario y del dispositivo.

Solución:

- Rockwell Automation se encuentra trabajando en la solución de estas vulnerabilidades y por el momento no hay solución. Para la vulnerabilidad de *cross-site scripting* recomienda utilizar las reglas IPS publicadas por CheckPoint en la pestaña «*Protection*».

Detalle:

- Una vulnerabilidad en la aplicación web del dispositivo afectado podría permitir a un atacante remoto sin autenticación la inyección de código arbitrario en el navegador web del usuario objetivo (XSS). Se ha asignado el identificador CVE-2019-19615 para esta vulnerabilidad.
- Un atacante remoto sin autenticación podría utilizar un *proxy* para habilitar cierta funcionalidad en la aplicación web del dispositivo que normalmente está disponible únicamente para usuarios de administración, pudiendo así modificar la configuración del usuario y del dispositivo. Se ha asignado el identificador CVE-2019-19616 para esta vulnerabilidad.

Etiquetas: 0day, Vulnerabilidad

Omisión de autenticación en Internet FAX ATA de Pangea Communications

Fecha de publicación: 15/02/2019

Importancia: Alta

Recursos afectados:

- Internet FAX Analog Telephone Adapter (ATA), versiones 3.1.8 y anteriores.

Descripción:

El investigador Ankit Anubhav, de NewSeky Security, ha reportado una vulnerabilidad de tipo omisión de autenticación que afecta a los dispositivos Internet FAX ATA de Pangea Communications. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto reiniciar el dispositivo causando una condición de denegación de servicio continua.

Solución:

- Pangea Communications ha contactado con los usuarios afectados y ha desarrollado un parche que soluciona esta vulnerabilidad.

Detalle:

- Un atacante podría evitar la autenticación enviando una URL especialmente diseñada y causar un reinicio en el dispositivo, lo que podría dar lugar a una condición de denegación de servicio continua. Se ha reservado el identificador CVE-2019-6551 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Schneider Electric

Fecha de publicación: 15/02/2019

Importancia: Alta

Recursos afectados:

- Vijeo Designer Lite V1.3SP1
- SoMachine Basic, todas las versiones
- Modicon M221, todas las versiones de firmware anteriores a V1.10.0.0
- Cámaras Pelco Sarix Enhanced de 1ª generacion:
  - Cámaras de interior:
    - IMES19-1I, IMES19-1S, IMES19-1P, IME119-1I, IME119-1S, IME119-1P , IME219-1I, IME219-1S, IME219-1P, IME319-1I, IME319-1S, IME319-1P, IME319-B1I, IME319-B1S, IME319-B1P, IME3122-1I, IME3122-B1I, IME3122-1S, IME3122-B1S, IME3122-1P, IME3122B1P
  - Cámaras ambientales:
    - IMES19-1EI, IMES19-1ES, IMES19-1EP, IME119-1EI, IME119-1ES, IME119-1EP, IME219-1EI, IME219-1ES, IME219-1EP, IME319-1EI, IME319-1ES, IME319-1EP, IME3122-1EI, IME3122-1ES, IME3122-1EP
  - Cámaras resistentes al vandalismo:
    - IMES19-1VI, IMES19-1VS, IMES19-1VP, IME119-1VI, IME119-1VS, IME119-1VP, IME219-1VI, IME219-1VS, IME219-1VP, IME319-1VI, IME319-1VS, IME319-1VP, IME3122-1VI, IME3122-1VS, IME3122-1VP
  - Cámaras de caja:
    - IXES1, IXE11, IXE21, IXE31
  - Cámaras Spectra Enhanced PTZ:
    - D6220, D6220L, D6230 y D6230L

Descripción:

Deng Yongkai de NSFOCUS, Gjoko Krstic de Zero Science, Matthias Niedermaier y Florian Fischer de Hochschule Augsburg, Jan-Ole Malchow de Freie Universität Berlin, Reid Wightman de Dragos Inc. y Schneider Electric han identificado varias vulnerabilidades, en los productos afectados, del tipo desbordamiento de búfer, permisos incorrectos, vulnerabilidades de entorno, inyección de comandos, XSS, CSRF y neutralización incorrecta de elementos especiales en consultas.

Solución:

- Vijeo Designer Lite: Está descontinuado desde junio de 2017. Para aquellos usuarios que requieran este producto, Schneider Electric aconseja que sea instalado en un sistema dedicado y con mínimos privilegios y accesos. Solo abrir proyectos DOP desde fuentes confiables.
- SoMachine Basic: Actualizar a la versión 1.0 de software (EcoStruxure Machine Expert ?Basic v 1.0)
- Modicon M221: Actualizar a la versión de firmware v1.10.0.0
- Cámaras Pelco Sarix Enhanced: Actualizar a la versión 2.2.3.0 de firmware.
- Cámaras Spectra Enhanced PTZ: Actualizar a la versión 2..11 o superior de firmware

Detalle:

Un usuario remoto malintencionado que aprovechara alguna de las vulnerabilidades descritas podría llegar a realizar las siguientes acciones en los productos afectados:

- ejecución de código,
- denegación de servicio,
- borrado de ficheros,
- conseguir acceso no autorizado.

Se han reservado los identificadores CVE-2018-7822, CVE-2018-7816, CVE-2018-7821, CVE-2018-7823, CVE-2018-7825, CVE-2018-7826, CVE-2018-7827, CVE-2018-7828 y CVE-2018-7829 para estas vulnerabilidades

Etiquetas: SCADA, Schneider Electric, Vulnerabilidad

Desbordamiento de búfer en gpsd y microjson de gpsd Open Source Project

Fecha de publicación: 15/02/2019

Importancia: Alta

Recursos afectados:

- Gpsd, versiones desde la 2.90 hasta la 3.17
- Microjson, versiones desde la 1.0 hasta la 1.3

Descripción:

GE Digital Cyber Security Services, en colaboración con GE-PSIRT, han reportado una vulnerabilidad de criticidad alta en gpsd y microjson de gpsd Open Source Project. Un atacante remoto podría ejecutar código, obtener información o provocar una situación de denegación de servicio.

Solución:

- Actualizar gspd a la versión 3.18
- Actualizar microjson a la versión 1.4

Detalle:

- Una vulnerabilidad del tipo desbordamiento de búfer basado en pila podría permitir a un atacante remoto, a través del puerto TCP 2947, ejecutar código de manera arbitraria, obtener información o generar una condición de denegación de servicio al desconectar el dispositivo. Se ha asignado el identificador CVE-2018-17937 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Validación de entradas inadecuada en Cscape de Horner Automation

Fecha de publicación: 20/02/2019

Importancia: Alta

Recursos afectados:

- Cscape 9.80 SP4 y anteriores.

Descripción:

Anonymous, trabajando con Zero Day Initiative de Trend Micro han identificado una vulnerabilidad de criticidad alta en productos Cscape de Horner Automation. Un atacante remoto podría ejecutar código u obtener información confidencial.

Solución:

- Actualizar Cscape a la versión 9.90. Puede descargarse en la web de Horner Automation.

Detalle:

Una incorrecta validación al procesar archivos POC, podría permitir a un atacante generar archivos especialmente modificados, que conllevaría a la revelación de información confidencial o la ejecución remota de código arbitrario. Se ha reservado el identificador CVE-2019-6555 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de lectura fuera de límites en CNCSoft de Delta Electronics

Fecha de publicación: 20/02/2019

Importancia: Media

Recursos afectados:

- CNCSoft ScreenEditor, versión 1.00.84 y anteriores.

Descripción:

Natnael Samson, trabajando con Zero Day Initiative de Trend Micro, ha identificado una vulnerabilidad de tipo lectura fuera de límites. Un atacante podría causar un desbordamiento de búfer que le permitiría divulgar información o bloquear la aplicación.

Solución:

- Actualizar CNCSoft ScreenEditor a la versión 1.01.15 y restringir la interacción con la ampliación a ficheros confiables.

Detalle:

- Una vulnerabilidad de lectura fuera de límites podría permitir a un atacante bloquear el software debido a la falta de validación de entrada del usuario para procesar los archivos de proyecto. Se ha reservado el identificador CVE-2019-6547 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en el servidor web de CODESYS afecta a múltiples productos

Fecha de publicación: 21/02/2019

Importancia: Crítica

Recursos afectados:

- CODESYS Control para BeagleBone, emPC-A/iMX6, IOT2000, Linux, PFC100, PFC200 y Raspberry Pi
- CODESYS Control RTE versión 3 y para Beckhoff CX
- CODESYS Control Win versión 3
- CODESYS HMI versión 3
- CODESYS Control versión 3 Runtime System Toolkit
- CODESYS versión 3 Embedded Target Visu Toolkit y Remote Target VisuToolkit

Descripción:

Ivan Cheyrezy, de Schneider Electric, ha identificado una vulnerabilidad de severidad crítica en múltiples productos CODESYS. Un atacante remoto podría ejecutar código, obtener información o generar una condición de denegación de servicio (DoS).

Solución:

- Actualizar los productos CODESYS afectados a la versión 3.5.14.10

Detalle:

- La vulnerabilidad en el servidor web es debida al procesar peticiones http o https que han sido específicamente generadas de forma malintencionada. Un atacante podría acceder a archivos fuera del directorio de trabajo mediante un salto de directorio. También es posible que el servidor web se paralice al generarse un desbordamiento de pila, que podría derivar en ejecución remota de código o una condición de denegación de servicio.

Etiquetas: Actualización, SCADA, Vulnerabilidad

Evasión de autenticación en controladores ILC GSM/GPRS de Phoenix Contact

Fecha de publicación: 27/02/2019

Importancia: Crítica

Recursos afectados:

- ILC 131 ETH
- ILC 131 ETH/XC
- ILC 151 ETH
- ILC 151 ETH/XC
- ILC 171 ETH 2TX
- ILC 191 ETH 2TX
- ILC 191 ME/AN
- AXC 1050

Descripción:

El investigador de seguridad Sergiu Sechel ha publicado un artículo en el que muestra una vulnerabilidad presente en los controladores ILC GSM/GPRS de Phoenix Contact en Internet. Un atacante remoto podría utilizar esta vulnerabilidad para realizar cambios en los dispositivos, obtener información sensible y originar denegaciones de servicio en las comunicaciones

Solución:

- Actualmente no hay actualización que mitigue la vulnerabilidad, se aconseja tener un control del puerto 1962/tcp que utiliza el protocolo PCWorx en los dispositivos afectados por la vulnerabilidad.

Detalle:

- La incorrecta autenticación en las sesiones TCP en el puerto 1962, podría permitir a un atacante remoto cambiar la configuración en los dispositivos afectados, obtener información sensible, originar una condición de denegación de servicio o saltar por el sistema de archivos mediante la función "*Create backup*". Se ha asignado el identificador CVE-2019-9201 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad