Boletín de enero de 2019

Avisos de Sistemas de Control Industrial

Evasión de autenticación por reinyección de tráfico en productos de Hetronic

Fecha de publicación: 04/01/2019

Importancia: Alta

Recursos afectados:

- Transmisores
  - Nova-M, todas las versiones anteriores a la r161
- Receptores
  - ES-CAN-HL, todas las versiones anteriores a Main r1864 y Estop_v24
  - BMS-HL, todas las versiones anteriores a Main r1175 y Estop_v24
  - MLC, todas las versiones anteriores a Main r1600 y Estop_v24
  - DC Mobile, todas las versiones anteriores a Main r515 y Estop_v24

Descripción:

Los investigadores Jonathan Andersson, Philippe Z Lin, Akira Urano, Marco Balduzzi, Federico Maggi, Stephen Hilt y Rainer Vosseler en colaboración con ZDI de Trend Micro, han reportado una vulnerabilidad de tipo evasión de autenticación al NCCIC. La explotación exitosa de esta vulnerabilidad, podría permitir a un atacante que tenga acceso a la red donde se encuentran los dispositivos afectados reinyectar tráfico y enviar mensajes arbitrarios o mantener un estado de ?stop? en los mismos.

Solución:

Hetronic recomienda a todos los clientes de Nova-M actualizar el firmware:

- Transmisores
  - Nova-M, actualizar a la versión r161
- Receptores
  - ES-CAN-HL, actualizar a la versión Main r1864 y Estop_v24
  - BMS-HL, actualizar a la versión Main r1175 y Estop_v24
  - MLC, actualizar a la versión Main r1600 y Estop_v24
  - DC Mobile, actualizar a la versión Main r515 y Estop_v24

Para solicitar una versión de firmware debe ponerse en contacto con Hetronic.

Detalle:

- Los dispositivos afectados utilizan códigos fijos que podrían permitir a un atacante reproducirlos mediante la captura y retransmisión de tráfico, siempre y cuando este se encuentre en la misma red que los dispositivos afectados. Esto permitiría a un atacante mediante la reinyección de paquetes, suplantar mensajes o mantener la carga controlada en un estado de ?stop? permanente. Se ha reservado el identificador CVE-2018-19023 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos Siemens

Fecha de publicación: 08/01/2019

Importancia: Crítica

Recursos afectados:

- SICAM A8000 CP-8000 y SICAM A8000 CP-802X, todas las versiones anteriores a V14

- SICAM A8000 CP-8050, todas las versiones anteriores a V2.00
- CP1604 y CP1616, todas las versiones anteriores a V2.8
- SIMATIC S7-300, todas las versiones anteriores a V3.X.16
- SIMATIC S7-1500 CPU, versiones anteriores a V1.8.5 y desde V2.0 hasta V2.5
- Firmware de IEC 61850 para módulos Ethernet EN100, todas las versiones anteriores a V4.33

Descripción:

Varios investigadores de la firma Positve y de Compass Security, han identificado varias vulnerabilidades que podrían permitir a un atacante generar una condición de denegación de servicio o monitorización de las comunicaciones internas.

Solución:

Siemens ha publicado las siguientes versiones de firmware que solucionan estas vulnerabilidades:

- SICAM A8000 CP-8000 y SICAM A8000 CP-802X, V14 o superior.
- SICAM A8000 CP-8050, V2.00 o superior.
- CP1604 y CP1616, V2.8 o superior.
- SIMATIC S7-300, V3.X.16 o superior.
- SIMATIC S7-1500 CPU, V2.5 o superior.
- Firmware de IEC 61850 para módulos Ethernet EN100, V4.33 o superior.

Detalle:

La explotación exitosa de alguna de estas vulnerabilidades podría derivar en:

- Cross-Site Scripting (XSS).
- Cross-Site Request Forgery (CSRF).
- Validación de datos inadecuada.
- Denegación de servicio (DoS).

Se han reservado los identificadores CVE-2018-13798, CVE-2018-13808, CVE-2018-13809, CVE-2018-13810, CVE-2018-16561, CVE-2018-16558 y CVE-2018-16559, y asignado los identificadores CVE-2018-11451 y CVE-2018-11452 para estas vulnerabilidades.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Confusión de tipos en CX-One de Omron

Fecha de publicación: 11/01/2019

Importancia: Media

Recursos afectados:

- CX-One, versiones 4.50 y anteriores que utilizan CX-Protocol con versiones 2.0 y anteriores.

Descripción:

Esteban Ruiz (mr_me) de Source Incite, trabajando con Zero Day Initiative de Trend Micro, han identificado una vulnerabilidad de confusión de tipo en CX-One de Omron. Un atacante podría ejecutar código con los privilegios de la aplicación.

Solución:

- Omron ha publicado la versión 2.01 de CX-Protocol para actualizar CX-One y solucionar esta vulnerabilidad. Esta actualización se encuentra disponible a través del servicio CX-One auto-update.

Detalle:

- Existen tres vulnerabilidades de confusión de tipos cuando se procesa el fichero de proyecto, un atacante podría crear un fichero de proyecto especialmente modificado para ejecutar código con los privilegios de la aplicación. Se ha reservado el identificador CVE-2018-19027 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Evasión de autenticación en DeltaV de Emerson

Fecha de publicación: 11/01/2019

Importancia: Alta

Recursos afectados:

- DeltaV DCS, versiones 11.3.1, 11.3.2, 12.3.1, 13.3.1, 14.3, R5.1, R6 y anteriores

Descripción:

El investigador Alexander Nochvay, de Kaspersky Lab, ha identificado una vulnerabilidad de tipo evasión de autenticación que afecta a los DCS DeltaV de Emerson. Un atacante podría cerrar un servicio y conseguir una denegación de servicio.

Solución:

- Emerson aconseja a todos los usuarios afectados aplicar los parches disponibles en el portal de soporte.

Detalle:

- Un atacante podría generar un script especialmente diseñado para evadir la autenticación del puerto de mantenimiento de un servicio pudiendo provocar una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2018-19021 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Almacenamiento de información sensible en claro en PNOZmulti Configurator de Pilz GmbH & Co. KG (Pilz)

Fecha de publicación: 11/01/2019

Importancia: Baja

Recursos afectados:

- PNOZmulti Configurator, todas las versiones anteriores a la 10.9

La vulnerabilidad del PNOZmulti Configurator afecta directamente al dispositivo PMI m107 diag HMI.

Descripción:

Gjoko Krstikj de Applied Risk ha identificado una vulnerabilidad de almacenamiento de información sensible en claro en el software PNOZmulti Configurator de Pilz. Un atacante con acceso local podría leer información sensible del sistema.

Solución:

El dispositivo PMI m107 diag HMI se encuentra obsoleto, la función afectada por la vulnerabilidad fue corregida en la versión 10.9 de PNOZmulti Configurator.

PILZ recomienda realizar las siguientes acciones correctivas:

- Para usuarios que no utilizan PMI m107 diag:
  - Instalar la versión 10.9 de PNOZmulti Configurator y borrar el contenido del directorio C:/Program-Data/Pilz/PNOZmulti Configurator v< version >/AppData/pmimicroconfig (reemplazar < versión > por la versión utilizada).
- A los usuarios de PMI m107 diag:
  - Continuar utilizando la versión antigua de PNOZmulti Configurator y proteger el PC frente a accesos no autorizados.

Detalle:

- Un atacante no autenticado con acceso local al sistema donde está instalado PNOZmulti Configurator podría ver datos de credenciales en texto en claro. Se ha reservado el identificador CVE-2018-19009 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Vulnerabilidad Cross-Site Scripting en Niagara de Tridium

Fecha de publicación: 11/01/2019

Importancia: Media

Recursos afectados:

- Niagara Enterprise Security 2.3u1, todas las versiones anteriores a 2.3.118.6
- Niagara AX 3.8u4, todas las versiones anteriores a 3.8.401.1
- Niagara 4.4u2, todas las versiones anteriores a 4.4.93.40.2
- Niagara 4.6, todas las versiones anteriores a 4.6.96.28.4

Descripción:

Los investigadores Daniel Santos y Elisa Constante, de SecurityMatters, han reportado una vulnerabilidad del tipo Cross-Site Scripting que afecta a los dispositivos Niagara de Tridium. Un atacante autenticado podría inyectar código en páginas web afectando a la confidencialidad.

Solución:

Tridium ha puesto a disposición de sus usuarios registrados actualizaciones específicas en función de los productos afectados. Pueden descargar las actualizaciones a través de los siguientes enlaces:

- Niagara Enterprise security 2.3u1, versión 2.3.118.6.
- Niagara AX 3.8u4, versión 3.8.401.1.
- Niagara 4.4u2, versión 4.4.93.40.2.
- Niagara 4.6, versión 4.6.96.28.4.

Detalle:

Un atacante remoto podría inyectar scripts en la parte de cliente de la página web, pudiendo ser visualizados por otros usuarios. Se ha reservado el identificador CVE-2018-18985 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de salto de directorio en Intelligent

Power Management de Eaton

Fecha de publicación: 17/01/2019

Importancia: Alta

Recursos afectados:

- Intelligent Power Management, versiones v1.62 y anteriores.

Descripción:

Eaton ha identificado una vulnerabilidad de tipo salto de directorio que afecta a su software Intelligent Power Management.

Solución:

- Eaton ha publicado la versión v1.64 del software que soluciona esta vulnerabilidad. Se recomienda a todos los clientes que utilizan el producto afectado, actualicen a dicha versión disponible en su centro de descargas.

Detalle:

- Un atacante podría aprovechar esta vulnerabilidad para obtener información del dispositivo. Se ha asignado el identificador CVE-2018-12031 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en X-320M de ControlByWeb

Fecha de publicación: 18/01/2019

Importancia: Alta

Recursos afectados:

- X-320M-I, versión de firmware v1.05 y anteriores.

Descripción:

John Elder y Tom Westenberg, de Applied Risk, han identificado dos vulnerabilidades que afectan a los dispositivos X-320M de ControlByWeb. Un atacante podría ejecutar código o provocar una denegación de servicio.

Solución:

- ControlByWeb ha publicado la versión 1.06 del firmware para solucionar estas vulnerabilidades.

Detalle:

- Un usuario autenticado podría realizar una configuración de red no válida, deteniendo así las comunicaciones basadas en TCP provocando una condición de denegación de servicio. Se ha reservado el identificador CVE-2018-18881 para esta vulnerabilidad.
- Una vulnerabilidad de tipo *cross-site scripting* (XSS), podría permitir a un usuario autenticado inyectar códigos arbitrarios y ejecutar códigos mediante el *setup.html* en la interfaz web. Se ha reservado el identificador CVE-2018-18882 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en CX-Supervisor de Omron

Fecha de publicación: 18/01/2019

Importancia: Alta

Recursos afectados:

- CX-Supervisor, versiones v3.42 y anteriores

Descripción:

Esteban Ruiz de Source Incite, trabajando con Zero Day Initiative de Trend Micro, ha identificado varias vulnerabilidades que afectan a CX-Supervisor de Omron. Un atacante podría ejecutar comandos con los privilegios en el contexto de la aplicación.

Solución:

- Omron ha publicado la versión 3.5.0.11 de CX-Supervisor que soluciona estas vulnerabilidades. Para protegerse adecuadamente, los proyectos de desarrollo deben ser actualizados y guardados en el nuevo formato, para posteriormente reconstruirlos en el formato de la versión 3.5.0.11

Detalle:

- La aplicación puede ejecutar código que haya sido inyectado en un archivo de proyecto. Un atacante podría explotar esta vulnerabilidad para ejecutar código con los privilegios de la aplicación. Se le ha asignado el identificador CVE-2018-19011.
- Un atacante podría crear un fichero de proyecto especialmente modificado con comandos inyectados para borrar y/o modificar archivos en el dispositivo. Se ha asignado el identificador CVE-2018-19013 para esta vulnerabilidad.

- Un atacante podría inyectar comandos para lanzar programas, crear, escribir y leer archivos en el dispositivo mediante un fichero de proyecto especialmente modificado. Se ha asignado el identificador CVE-2018-19015 para esta vulnerabilidad.
- Un atacante podría utilizar un fichero de proyecto especialmente modificado, para aprovecharse de un fallo en la verificación de liberación de la memoria de la aplicación, y de este modo ejecutar código con los privilegios de la aplicación. Se ha asignado el identificador CVE-2018-19017 para esta vulnerabilidad.
- Un atacante podría utilizar un fichero de proyecto especialmente modificado y aprovecharse de varias confusiones de tipo para explotar y ejecutar código con los privilegios de la aplicación. Se ha asignado el identificador CVE-2018-19011 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Facility Explorer de Johnson Controls

Fecha de publicación: 23/01/2019

Importancia: Crítica

Recursos afectados:

- Facility Explorer versiones 14.X anteriores a la versión 14.4u1
- Facility Explorer versiones 6.X anteriores a la 6.6

Descripción:

Tridium identificó múltiples vulnerabilidades que afectan a los productos de automatización Facility Explorer de Johnson Controls. Un atacante podría acceder al sistema aprovechando una gestión incorrecta de las contraseñas y obtener acceso a los ficheros para su lectura, modificación, eliminación e incluso obtener permisos de administrador.

Solución:

Johnson Controls ha mitigado estas vulnerabilidades en versiones posteriores del producto. Los usuarios deben actualizar sus versiones a una segura, se recomienda la versión (FX14.6).

- Facility Explorer 14.6 (Fecha de lanzamiento septiembre 2018).
- Facility Explorer 14.4u1 (Fecha de lanzamiento agosto 2018).
- Facility Explorer 6.6 (Fecha de lanzamiento agosto 2018).

Detalle:

- Un atacante con acceso al sistema Facility Explorer y permisos de administrador, podría realizar una vulnerabilidad del tipo de salto de directorio (?path traversal?), para acceder a ficheros sin permisos o directorios restringidos. Se ha asignado el identificador CVE-2017-16744 para esta vulnerabilidad.
- Un fallo en las cuentas de usuario deshabilitadas con el campo contraseña en blanco, podría permitir a un atacante acceder al sistema con permisos de administrador. Se ha asignado el identificador CVE-2017-16748 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en dispositivos DIVAR 400 & 600 de Bosch

Fecha de publicación: 23/01/2019

Importancia: Crítica

Recursos afectados:

- DIVAR 400 & 600 series, todas las versiones.

Descripción:

El investigador independiente Maxim Rupp ha reportado dos vulnerabilidades que afectan a los dispositivos DIVAR 400 & 600 de Bosch. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto obtener información sin autenticación y obtener credenciales del dispositivo.

Solución:

- Bosch recomienda operar los dispositivos en una red cerrada, si esto no es posible, aconseja sustituir los dispositivos por la última versión de DIVAR, ya que no presenta estas vulnerabilidades.

Detalle:

- Un atacante remoto podría ser capaz de obtener información de la aplicación accediendo a una dirección URL específica del servidor web embebido del dispositivo.
- Las contraseñas se encuentran almacenadas en un fichero accesible sin autenticación. Además, las credenciales de administrador podrían ser obtenidas por un atacante mediante la inyección XML de código shell.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en Infinity Delta de

Dräger

Fecha de publicación: 23/01/2019

Importancia: Alta

Recursos afectados:

- Dräger Infinity® Delta, Delta XL y Kappa, todas las versiones.
- Dräger Infinity® Explorer C700, todas las versiones.

Descripción:

Los investigadores Marc Ruef y Rocco Gagliardi de scip AG han identificado múltiples vulnerabilidades que afectan a los dispositivos Infinity Delta de Dräger. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto la divulgación de la información, el escalado de privilegios o provocar una condición de denegación de servicio.

Solución:

- Dräger ha publicado la versión Delta/Infinity Explorer VF10.1 para solucionar estas vulnerabilidades, que puede ser descargada mediante ServiceConnect de Dräger.

Detalle:

- El envío de un paquete de red malformado podría causar un reinicio en el monitor, debido a una validación inadecuada de los datos de entrada. Si se envía de forma repetida, un atacante podría ser capaz de interrumpir la monitorización del paciente haciendo que el monitor se reinicie repetidamente hasta que vuelva a la configuración predeterminada y pierda la conectividad de red. Se ha reservado el identificador CVE-2018-19010 para esta vulnerabilidad.
- Los ficheros de log son accesibles mediante una conexión de red sin autenticación. Un atacante podría obtener información sobre los componentes internos del monitor del paciente, la ubicación del monitor y la configuración de la red por cable. Se ha reservado el identificador CVE-2018-19014 para esta vulnerabilidad.
- Un atacante podría salir del modo quiosco mediante un diálogo específico y obtener control del sistema operativo. Se ha reservado el identificador CVE-2018-19012 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en switches FL de PHOENIX CONTACT

Fecha de publicación: 24/01/2019

Importancia: Alta

Recursos afectados:

- Switches FL 3xxx, 4xxx y 48xx, versiones desde 1.0 hasta 1.34

Descripción:

Evgeniy Druzhinin, Ilya Karpov y Georgy Zaytsev, de Positive Technologies, han identificado varias vulnerabilidades de tipo CSRF, restricción inadecuada de excesivos intentos de autenticación, transmisión en claro, consumo de recursos no controlado, almacenamiento inseguro de información sensible y errores de búfer que afectan a los switches FL de PHOENIX CONTACT. Un atacante remoto podría obtener acceso al equipo, identificar contraseñas, ejecutar una denegación de servicio (DoS) o realizar un MitM (*Man in the Middle*).

Solución:

- PHOENIX CONTACT recomienda a todos los usuarios habilitar la seguridad del protocolo HTTP y actualizar a la versión 1.35 o superior de *firmware*.

Detalle:

- CSRF: un atacante podría persuadir a un usuario para que siga un enlace malicioso, lo que le permitiría enviar peticiones arbitrarias al software afectado a través del navegador web del usuario con sus privilegios. Se ha reservado el identificador CVE-2018-13993 para esta vulnerabilidad.
- Restricción inadecuada: el switch necesita una funcionalidad extendida de tiempo de espera (time-out) de inicio de sesión para evitar una rápida combinación de nombres de usuario y contraseñas automatizadas. Un atacante obtendría acceso mediante un ataque de fuerza bruta a las credenciales. Se ha reservado el identificador CVE-2018-13990 para esta vulnerabilidad.
- Transmisión en claro: la configuración por defecto permite que la contraseña se transmita en claro, un atacante podría leerla haciendo una captura de tráfico. Se ha reservado el identificador CVE-2018-13992 para esta vulnerabilidad.
- Consumo de recursos no controlado: un atacante remoto podría provocar una condición de denegación de servicio si inicia demasiadas conexiones con la Web. Se ha reservado el identificador CVE-2018-13994 para esta vulnerabilidad.
- Almacenamiento inseguro: un atacante podría extraer las claves primarias de los certificados de una imagen del *firmware*. Se ha reservado el identificador CVE-2018-13991 para esta vulnerabilidad.
- Errores de búfer: cuando se utiliza la configuración HTTPS puede darse un error de precisión en la lectura del certificado que provocar que no se muestre correctamente. Se ha asignado el identificador CVE-2017-3735 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en WebAccess/SCADA de Advantech

Fecha de publicación: 25/01/2019

Importancia: Crítica

Recursos afectados:

- WebAccess/SCADA, versión 8.3

Descripción:

Devesh Logendran, de Attila Cybertech Pte. Ltd., ha identificado varias vulnerabilidades de tipo autenticación inadecuada, evasión de autenticación e inyección SQL que afectan al software WebAccess/SCADA de Advantech. Un atacante local podría acceder y modificar datos sensibles.

Solución:

- Advantech ha publicado la versión 8.3.5 de WebAccess/SCADA que soluciona estas vulnerabilidades.

Detalle:

Un atacante podría:

- Conseguir una evasión de autenticación y cargar datos maliciosos de manera remota. Se ha reservado el identificador CVE-2019-6519 para esta vulnerabilidad.
- Realizar peticiones especialmente modificadas para conseguir evadir la autenticación y obtener o modificar datos sensibles. Se ha reservado el identificador CVE-2019-6521 para esta vulnerabilidad.
- Aprovechar las entradas SQL no validadas adecuadamente. Se ha reservado el identificador CVE-2019-6523 para esta vulnerabilidad.

Etiquetas: Actualización, SCADA, Vulnerabilidad

Control de acceso inadecuado en License Manager de Yokogawa

Fecha de publicación: 25/01/2019

Importancia: Alta

Recursos afectados:

- CENTUM VP Y CENTUM VP Entry Class, versiones R5.01.00 y R6.06.00.
- ProSafe-RS, versiones R3.01.00 y R4.04.00.
- PRM, versiones R4.01.00 y R4.02.00.
- B/M9000 VP, versiones R7.01.01 y R8.02.03.

Descripción:

Yokogawa, en colaboración con Kaspersky Lab, ha identificado una vulnerabilidad de tipo control de acceso inadecuado en License Manager que afecta a varios de sus productos. Un potencial atacante remoto podría ejecutar código malicioso.

Solución:

Yokogawa sugiere las siguientes actualizaciones para cada uno de sus productos:

- CENTUM VP y CENTUM VP Entry Class:
  - R5.01.00 a R5.04.00: actualizar a R5.04.20 y aplicar el parche R5.04.C5.
  - R5.04.20: aplicar el parche R5.04.C5.
  - R6.01.0 a R6.05.00: actualizar a R6.06.03.
- ProSafe-RS
  - R3.01.00 a R3.02.10: actualizar a la versión R3.02.20 y aplicar el parche R3.02.38.
  - R3.02.20: aplicar el parche R3.02.38.
  - R4.01.00 a R4.03.10: actualizar a la versión R3.04.00 y aplicar el parche R4.04.01
  - R4.04.00: aplicar el parche R4.04.01.
- PRM, actualizar a la versión R4.02.00 y aplicar el parche R4.02.01.
- B/M9000 VP, actualizar CENTUM VP si está instalado en la misma máquina que B/M9000 VP.

Detalle:

- Esta vulnerabilidad puede permitir a los atacantes remotos crear o invalidar cualquier archivo, en cualquier lugar con privilegios de sistema, en el ordenador en el que se ejecuta el servicio License Manager. Existe el riesgo de que si los atacantes remotos utilizan esta vulnerabilidad, puedan obstaculizar las funciones de ese equipo, etc. No se dispone de CVE para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Posible acceso no autorizado en Wonderware System Platform de Aveva

Fecha de publicación: 28/01/2019

Importancia: Alta

Recursos afectados:

- Wonderware System Platform 2017 Update 2 y versiones anteriores.

Descripción:

Vladimir Dashchennko de Kaspersky Lab, ha reportado una vulnerabilidad en Wonderware System Platform de Aveva debida a unas credenciales insuficientemente protegidas.

Solución:

Aveva recomienda a todos los usuarios afectados actualizar a la Update 3 que soluciona esta vulnerabilidad. La actualización se encuentra disponible para los usuarios registrados a través del siguiente enlace:

- https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=52332

Detalle:

- El sistema emplea una cuenta de usuario de red ArchestrA para la autenticación de procesos del sistema y las comunicaciones entre nodos. Un atacante no autorizado podría hacer uso de la API para obtener las credenciales de la cuenta.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en LeviStudio de Wecon Technology

Fecha de publicación: 30/01/2019

Importancia: Crítica

Recursos afectados:

- LeviStudioU

Descripción:

Los investigadores Natnael Samson, Ziad Badawi y Mat Powell, de Zero Day Initiative (ZDI), han identificado varias vulnerabilidades de tipo desbordamiento de búfer y corrupción de memoria.

Solución:

No existe solución publicada para estas vulnerabilidades.

- ZDI propone como medida de prevención que los productos afectados interactúen únicamente con ficheros de confianza.

Detalle:

- No se valida correctamente la longitud de los datos proporcionados por el usuario antes de copiarlos en el búfer, esto podría originar un desbordamiento del mismo y permitiría a un atacante ejecutar código arbitrario.
- Las cadenas leídas en la entrada no son verificadas correctamente, esto podría provocar una corrupción de memoria y permitiría a un atacante ejecutar código de forma remota.

Etiquetas: 0day, Vulnerabilidad

Reutilización de Nonce en camas articuladas de Stryker

Fecha de publicación: 30/01/2019

Importancia: Media

Recursos afectados:

- Secure II MedSurg Bed (habilitada con iBed Wireless), modelo 3002.
- S3 MedSurg Bed (habilitada con iBed Wireless), modelos 3002 S3 y 3005 S3.
- InTouch ICU Bed (habilitada con Bed Wireless), modelos 2131 y 2141.

Descripción:

Mathy Vanhoef de imec-DistriNet, KU Leuven, identifico la vulnerabilidad KRACK que Stryker ha notificado. Un atacante podría manipular los datos de tráfico consiguiendo la divulgación de las comunicaciones cifradas o la inyección de datos.

Solución:

- Gateway 1.0 ? No hay parche disponible
- Gateway 2.0 ? Actualizar a la versión 5212-400-905_3.5.002.01
- Gateway 3.0 ? Actualizado en la versión actual de software: 5212-500-905_4.3.001.01

Además, Stryker recomienda:

- Deshabilitar la conexión Wireless iBed cuando no sea necesaria.
- Que sus productos se encuentren en una red aislada y posean segmentación propia.

Detalle:

- Un potencial atacante podría manipular el tráfico del establecimiento de sesión en 4 pasos en comunicaciones wifi con protección WPA y WPA2 gracias al ataque KRACK y llevar a cabo un ataque de tipo Man in the Middle, pudiendo repetir, descifrar o robar tramas. Se han asignado los identificadores CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087 y CVE-2017-13088 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad de denegación de servicio en PLC de la serie MELSEC-Q de Mitsubishi Electric

Fecha de publicación: 30/01/2019

Importancia: Alta

Recursos afectados:

PLC MELSEC-Q de las series:

- Q03/04/06/13/26UDVCPU y Q04/06/13/26UDPVCPU con número de serie 20081 y anteriores.
- Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU con número de serie 20101 y anteriores.

Descripción:

Tri Quach del grupo Customer Fulfillment Technology Security (CFTS) de Amazon ha identificado una vulnerabilidad de tipo consumo de recursos no controlado en los PLC de la serie MELSEC-Q de Mitsubishi Electric. Un atacante remoto podría enviar bytes específicos al dispositivo consiguiendo que la comunicación Ethernet se pare.

Solución:

- Mitsubishi Electric ha publicado una nueva versión del firmware para los productos afectados. Además, recomienda que los productos afectados se situen detrás de un cortafuegos.

Detalle:

- Un atacante remoto podría enviar paquetes al puerto 5007 con la consecuencia de un error en la pila Ethernet. Se ha asignado el identificador CVE-2019-6535 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad