Boletín de Mayo de 2018

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en productos de Siemens

Fecha de publicación: 03/05/2018

Importancia: Alta

Recursos afectados:

- Siveillance VMS 2016 R y anteriores, todas las versiones anteriores a la V10.0a
- Siveillance VMS 2016 R2, todas las versiones anteriores a la V10.1a
- Siveillance VMS 2016 R3, todas las versiones anteriores a la V10.2b
- Siveillance VMS 2017 R1, todas las versiones anteriores a la V11.1a
- Siveillance VMS 2017 R2, todas las versiones anteriores a la V11.2a
- Siveillance VMS 2018 R1, todas las versiones anteriores a la V12.1a
- Siveillance VMS Video para Android e iOS, todas las versiones anteriores a la V12.1a (2018 R1)
- SINAMICS GH150 V4.7 w. PROFINET, todas las versiones anteriores a la V4.7 SP5 HF7
- SINAMICS SL150 V4.7.0 w. PROFINET, todas las versiones anteriores a la V4.7 HF30
- SINAMICS GL150 V4.7 w. PROFINET, SINAMICS GM150 V4.7 w. PROFINET, SINAMICS SL150 V4.7.4 w. PROFINET, SINAMICS SL150 V4.7.5 w. PROFINET y SINAMICS SM120 V4.7 w. PROFINET. Todas las versiones anteriores a la V4.8 SP2
- SINAMICS SM150 V4.7 w. SIMOTION y PROFINET. Todas las versiones

Descripción:

El investigador Karsten Sohr de TZI Bremen ha descubierto las vulnerabilidades relacionadas con el producto Siveillance VMS Video Mobile App para Android y IOS, que permitirían a un atacante leer o escribir datos, en el canal de comunicación cifrado entre la App y el servidor. Las otras vulnerabilidades que afectan a SINAMICS y Siveillance VMS permitirían a un atacante una elevación de privilegios y/o causar una Denegación de Servicio.

Solución:

Siemens ha desarrollado actualizaciones de software para solucionar las vulnerabilidades que afectan a sus productos. A continuación, se listan los productos y sus correspondientes actualizaciones:

- Siveillance VMS 2016 R y anteriores ? Actualizar a la versión 10.0a
- Siveillance VMS 2016 R2 ? Actualizar a la versión 10.1a
- Siveillance VMS 2016 R3 ? Actualizar a la versión V10.2b
- Siveillance VMS 2017 R1 ? Actualizar a la versión V11.1a
- Siveillance VMS 2017 R2 ? Actualizar a la versión V11.2a
- Siveillance VMS 2018 R1 ? Actualizar a la versión V12.1a

Visite el siguiente enlace para descargar la actualización correspondiente a su producto: https://psp.sbt.siemens.com/

AdemÃis, como recomendación genérica a aplicar, el fabricante aconseja restringir el acceso de red por los puertos 7474/TCP y el puerto 9993/TCP a los productos Siveillance VMS.

- Siveillance VMS Video para Android e iOS: Actualizar a la versión V12.1a (2018 R1) (https://play.google.com/store/apps/details?id=com.siemens.siveillancevms, https://itunes.apple.com/us/app/siveillance-vms-video/id1045047239)
- SINAMICS GH150 V4.7 w. PROFINET y SINAMICS SL150 V4.7.0 w. PROFINET: Actualizar a la versión V4.7 SP5 HF7 o cambiar a la versión V4.8 SP2
- SINAMICS GL150 V4.7 w. PROFINET, SINAMICS GM150 V4.7 w. PROFINET, SINAMICS SL150 V4.7.4 w. PROFINET, SINAMICS SL150 V4.7.5 w. PROFINET y SINAMICS SM120 V4.7 w. PROFINET: Actualizar a la versión V4.8 SP2
- SINAMICS SM150 V4.7 w. SIMOTION y PROFINET
  - Aplicar la protección de red e implementar defensa en profundidad.
  - Proteger el acceso de red por el puerto 161/TCP a los productos afectados.
  - Uso de servicios VPN para proteger las comunicaciones entre redes.

Detalle:

- Escalada de privilegios y/o denegación de servicio en el producto Siveillance VMS: Diverso software de Siveillance VMS de

Siemens dispone de una vulnerabilidad debido a una incorrecta deserialización. Un atacante local puede explotar esta vulnerabilidad para elevar privilegios o causar una denegación de servicio. Se ha reservado un código CVE-2018-7891 para esta vulnerabilidad.
- Denegación de servicio en el producto SINAMICS: Un potencial atacante en red local podría enviar paquetes broadcast PROFINET especialmente manipulados que podrían causar una condición de denegación de servicio de los productos afectados. Se requiere la intervención de un operador para recuperar el sistema. Se ha reservado el identificador CVE-2017-2680 para esta vulnerabilidad.
- Denegación de servicio en el producto SINAMICS: Un potencial atacante en red local podría enviar paquetes al puerto 161/UDP especialmente manipulados que podrían causar una condición de denegación de servicio de los productos afectados. Los productos afectados deben reiniciarse de forma manual. Se ha reservado el identificador CVE-2017-12741 para esta vulnerabilidad.
- Divulgación de información en el producto Siveillance VMS Video Mobile App: La validación inadecuada de un certificado podría permitir a un potencial atacante privilegiado leer y escribir datos en el canal de datos cifrado entre la aplicación y el servidor, interceptar la comunicación mediante un ataque Man-in-the-Middle y/o generar un certificado derivado del algoritmo de validación igual que al aceptado. Se ha reservado el identificador CVE-2018-4849 para esta vulnerabilidad.

Etiquetas: iOS, Móviles, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en IDS 2012 de Lantech

Fecha de publicación: 04/05/2018

Importancia: Crítica

Recursos afectados:

- IDS 2012 versión 2.0 y anteriores.

Descripción:

El investigador Florian Adamsky ha identificado múltiples vulnerabilidades que afectan al producto IDS 2012 de Lantech. Un potencial atacante remoto, podría explotar estas vulnerabilidades para ejecutar código remoto en el sistema debido a una incorrecta validación de los campos de entrada.

Solución:

Lantech no ha proporcionado ninguna solución a estas vulnerabilidades.

Detalle:

- Incorrecta validación de campos de entrada: La mayoría de los campos de entrada en el producto afectado no disponen de una correcta validación de los mismos. Se ha asignado el código CVE-2018-8869 para esta vulnerabilidad.
- Desbordamiento de Búfer que permitiría a un potencial atacante ejecutar código de forma remota. Se ha asignado el código CVE-2018-8865 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en escáneres Brilliance CT de Philips

Fecha de publicación: 04/05/2018

Importancia: Alta

Recursos afectados:

- Brilliance 64 versiones 2.6.2 y anteriores
- Brilliance iCT versiones 4.1.6 y anteriores
- Brillance iCT SP versiones 3.2.4 y anteriores
- Brilliance CT Big Bore versiones 2.3.5 y anteriores

Descripción:

Philips ha informado de 3 vulnerabilidades, 1 de ellas de severidad alta, de tipo ejecución con privilegios innecesarios, exposición de recursos y uso de credenciales embebidas que afectan a escÃineres de Tomografías computerizadas (CT) Brilliance y que podrían permitir a un atacante impactar en la confidencialidad, integridad y disponibilidad en los sistemas afectados.

Solución:

Philips ha identificado la siguiente guía y control de mitigación de riesgos:

> Los usuarios deben operar todos los productos Brilliance CT instalados y compatibles de Philips dentro de las especificaciones autorizadas de Philips, incluido el software aprobado por Philips, la configuración del software, los servicios del sistema y la configuración de seguridad, como las operaciones de los cortafuegos. Philips también recomienda a los usuarios que implementen una estrategia de defensa en profundidad para proteger sus sistemas contra amenazas de seguridad internas y externas, incluyendo restringir el acceso físico al escÃiner a solo el personal autorizado, reduciendo así el riesgo de que un acceso físico pueda ser comprometido por un usuario no autorizado.

Philips también ha solucionado las vulnerabilidades de credenciales embebidas para Brilliance iCT 4.x y versiones anteriores. Las Instrucciones de uso (IFU) de la familia Philips iCT-iPatient (v4.x) hacen referencia a la capacidad de administrar credenciales y se puede acceder desde el Philips InCenter en https://incenter.medical.philips.com para usuarios con derechos.

Detalle:

- Ejecución con privilegios innecesarios: los dispositivos afectados operan las funciones del usuario desde un kiosco contenido en un sistema operativo Microsoft Windows. Windows arranca de forma predeterminada con privilegios elevados, lo que permite que una aplicación, usuario o potencial atacante, logre potencialmente privilegios elevados no autorizados. AdemÃis, los atacantes pueden obtener acceso a recursos no autorizados de Windows. Se ha reservado el identificador CVE-2018-8853 para esta vulnerabilidad.

- Exposición de recursos: un usuario con acceso limitado o un atacante no autorizado podría salir de la contención del entorno del kiosco, obtener privilegios elevados del sistema y acceder a recursos no autorizados del sistema operativo. Se ha reservado el identificador CVE-2018-8861 para esta vulnerabilidad.
- Uso de credenciales embebidas: el software contiene credenciales fijas, como contraseñas o claves criptogrÃificas, que utiliza para su propia autenticación de entrada, comunicación de salida a componentes externos o cifrado de datos internos. Un potencial atacante podría comprometer estas credenciales y obtener acceso al sistema. Se ha reservado el identificador CVE-2018-8857 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en productos de Silex Technology y GE Healthcare

Fecha de publicación: 09/05/2018

Importancia: Alta

Recursos afectados:

- GEH-500 Versión 1.54 y anteriores
- SX-500 todas las versiones. (Discontinuado desde 2011)
- GEH-SD-320AN versión GEH-1.1 y anteriores
- SD-320AN versión 2.01 y anteriores. (Discontinuada desde noviembre de 2017)
- GE MAC Resting ECG Modelo MAC 3500
- GE MAC Resting ECG Modelo MAC 5000. (Discontinuado desde 2012)
- GE MAC Resting ECG Modelo MAC 5500
- GE MAC Resting ECG Modelo MAC 5500 HD

Descripción:

El investigador Eric Evenchick de Atredis Partners ha identificado múltiples vulnerabilidades que afectan a los productos de Silex Technology y GE Healthcare. Un potencial atacante remoto, podría explotar estas vulnerabilidades para modificar las configuraciones del sistema o ejecutar código de forma remota.

Solución:

Silex Technology y GE Healthcare recomiendan las siguientes mitigaciones:

- CVE-2018-6020 (GE MobileLink/SX-500): Habilitar la cuenta ?Update?, en la interfaz web, que viene deshabilitada por defecto. Configurar una segunda contraseña en dicha cuenta ?Update?, para prevenir la realización de cambios de configuración, sin autenticar, en el dispositivo.
- CVE-2018-6021 (GE MobileLink/GEH-SD-320AN): Silex Technology y GE Healthcare han desarrollado una actualización para solucionar la vulnerabilidad, que serÃi descargable, una vez testeada, a partir del 31 de mayo del 2018.

Detalle:

- Autenticación Incorrecta: La autenticación en el sistema no es verificada de manera correcta para ciertas peticiones POST, esto permitiría a un atacante modificar ciertas configuraciones del sistema. Se ha asignado el código CVE-2018-6020 para esta vulnerabilidad.
- Validación incorrecta de parÃimetros en las llamadas a sistema: Los parÃimetros utilizados en llamadas a Sistema, no son correctamente sanitizados, lo que permitiría a un posible atacante la ejecución de código inyectando comandos en estos parÃimetros. Se ha asignado el código CVE-2018-6021 para esta vulnerabilidad

Etiquetas: Vulnerabilidad

Falta de control en acceso a ficheros o directorios en MatrikonOPC Explorer de MatrikonOPC

Fecha de publicación: 11/05/2018

Importancia: Media

Recursos afectados:

- MatrikonOPC Explorer versión 5.0 y anteriores

Descripción:

El investigador Ilya Kapov de Positive Technologies ha reportado esta vulnerabilidad relacionada con la falta de control en el acceso a ficheros o directorios. Un atacante con acceso local al sistema podría explotar esta vulnerabilidad, permitiendo al mismo, transferir ficheros sin autorización desde el sistema anfitrión. Este hecho, podría dar lugar a una divulgación de información.

Solución:

MatrikonOPC ha publicado un parche que soluciona esta vulnerabilidad. El siguiente enlace permite acceder a la descarga del parche:

https://www.matrikonopc.com/downloads/176/software/index.aspx

Detalle:

- Vulnerabilidad de archivos o directorios accesibles para terceros: Una explotación exitosa de esta vulnerabilidad podría permitir a un atacante con acceso local transferir ficheros sin autorización desde el sistema anfitrión. Se ha asignado el código CVE-2018-8714 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Rockwell Automation

Fecha de publicación: 11/05/2018

Importancia: Crítica

Recursos afectados:

- Arena versiones 15.10.00 y anteriores
- FactoryTalk Activation Manager v4.00 y v4.01, distribuido en Wibu-Systems CodeMeter v6.50b y anteriores
- FactoryTalk Activation Manager v4.00 y anteriores, distribuido con FlexNet Publisher v11.11.1.1 y anteriores
- Notar que los siguientes productos requieren el uso de FactoryTalk Activation Manager:
  - Arena
  - Emonitor
  - FactoryTalk AssetCentre
  - FactoryTalk Batch
  - FactoryTalk EnergyMetrix
  - FactoryTalk eProcedure
  - FactoryTalk Gateway
  - FactoryTalk Historian Classic
  - FactoryTalk Historian Site Edition (SE)
  - FactoryTalk Information Server
  - FactoryTalk Metrics
  - FactoryTalk Transaction Manager
  - FactoryTalk VantagePoint
  - FactoryTalk View Machine Edition (ME)
  - FactoryTalk View Site Edition (SE)
  - FactoryTalk ViewPoint
  - RSFieldBus
  - RSLinx Classic
  - RSLogix 500
  - RSLogix 5000
  - RSLogix5
  - RSLogix Emulate 5000
  - RSNetWorx
  - RSView32
  - SoftLogix 5800
  - Studio 5000 Architect
  - Studio 5000 Logix Designer
  - Studio 5000 Logix Emulate
  - Studio 5000 View Designer

Descripción:

Rockwell Automation y el investigador Ariele Caltabiano en colaboración con Zero Day Initiativede Trend Micro, han identificado varias vulnerabilidades en las que un potencial atacante con acceso a los dispositivos afectados podría llegar acceder a información sensible, sobrescribir contenido, realizar una denegación de servicio o provocar un desbordamiento de búfer pudiendo llegar a ejecutar código de forma remota.

Solución:

Rockwell Automation recomienda a los usuarios con versiones afectadas de CodeMeter o FlexNet Publisher que han sido instalados con Factory Talk Activation Manager actualizar a la versión v4.02. Si no es posible actualizar directamente la versión de Factory Talk Activation Manager v4.02, se debería previamente actualizar CodeMeter a una versión que soporte dicha actualización.

Los usuarios de Arena Software disponen de versiones actualizadas v15.10.01 y posteriores, que corrigen estas vulnerabilidades, que pueden descargarse en el siguiente enlace (Acceso privado):
https://rockwellautomation.custhelp.com/app/answers/detail/a_id/1073588

Rockwell Automation recomienda aplicar otras medidas de seguridad adicionales a las propias actualizaciones:

- Bloquear todo el trÃifico Ethernet/IP u otros protocolos basados en CIP, donde no sea estrictamente necesario. Los puertos que deben tener un acceso restringido son puerto TCP/2222 y UDP/44818. Se recomienda utilizar medias de control de trÃifico como cortafuegos, dispositivos UTM, etc.
- Minimizar la exposición de los dispositivos y asegurar que no estén accesibles desde Internet.
- Realizar los accesos remotos con métodos seguros, como son el uso de VPN (Virtual Private Networks).

Detalle:

- Cross-Site-Scripting (?XSS?): un potencial atacante local, podría aprovechar una vulnerabilidad en Wibu-Systems CodeMeter para inyectar scritps web o código HTML, aprovechando un campo en el fichero de configuración. Esta vulnerabilidad permitiría a dicho atacante acceder a información sensible o reescribir el contenido de la pÃigina HTML. Se ha asignado el código CVE-2017-13754 para esta vulnerabilidad.

- Incorrecta restricción de operaciones dentro de los límites de la memoria del buffer: una función propietaria encargada de copiar las cadenas dentro de FlexNet Publisher, no vÃilida de manera adecuada los datos de entrada, permitiendo a un potencial atacante, sin necesidad de estar autenticado, enviar mensajes especialmente modificados para causar un desbordamiento de búfer. Se ha asignado el código CVE-2015-8277 para esta vulnerabilidad.

- Incorrecta liberación de memoria: el uso de memoria sin que esta sea previamente liberada de manera correcta, podría ser aprovechada por un potencial atacante para enviar paquetes especialmente malformados, causando a la aplicación un estado inestable, pudiendo afectar a la disponibilidad o la pérdida de datos no guardados. Se ha asignado el código CVE-2018-8843 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Gestión incorrecta de paquetes en SIMATIC S7-400 de Siemens

Fecha de publicación: 15/05/2018

Importancia: Alta

Recursos afectados:

- SIMATIC S7-400 con versión 4.0 de hardware y anteriores, todas las versiones
- SIMATIC S7-400 con versión 5.0 de hardware, todas las versiones de firmware anteriores a la V5.2
- SIMATIC S7-400H con versión 4.5 de hardware y anteriores, todas las versiones

Descripción:

Siemens ha identificado una vulnerabilidad de gestión incorrecta de paquete malformados en dispositivos SIMATIC S7-400. Un potencial atacante podría conseguir una denegación de servicio del producto afectado.

Solución:

Siemens aconseja a todos los usuarios actualizar a las siguientes versiones:

- SIMATIC S7-400 con versión 4.0 de hardware y anteriores: Actualizar a la versión 5.0 de hardware, disponible en https://support.industry.siemens.com/cs/ww/en/view/109483507
- SIMATIC S7-400 con versión 5.0 de hardware: Actualizar a la versión de firmware V5.2 o superior, disponible en https://support.industry.siemens.com/cs/ww/en/view/109474827
- SIMATIC S7-400H con versión 4.5 de hardware y anteriores: Actualizar a la versión 6.0 de hardware, disponible en https://support.industry.siemens.com/cs/ww/en/view/75407031

Detalle:

Los productos afectados validan de manera inadecuada los paquetes de comunicaciones S7, lo que podría causar una denegación de servicio que requiere de un reinicio manual. Un potencial atacante podría enviar paquetes S7 especialmente malformados al interfaz de comunicación de la CPU, incluyendo las interfaces Ethernet, PROFIBUS y Multi Point Interfaces (MPI). Se ha reservado el código CVE-2018-4850 para esta vulnerabilidad

Etiquetas: Actualización, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en WebAccess de Advantech

Fecha de publicación: 16/05/2018

Importancia: Crítica

Recursos afectados:

- WebAccess versión 8.2_20170817 y anteriores
- WebAccess versión 8.3.0 y anteriores
- WebAccess Dashboard versión 2.0.15 y anteriores
- WebAccess Scada Node versiones anteriores a 8.3.1
- WebAccess/NMS versión 2.0.3 y anteriores

Descripción:

Varios investigadores trabajando con Trend Micro?s Zero Day Initiative han reportado una serie de vulnerabilidades cuya explotación podría permitir a un atacante divulgar información sensible del host y/o destino, ejecutar código arbitrario o eliminar archivos.

Solución:

Advantech ha publicado un parche que soluciona esta vulnerabilidad, disponible en http://support.advantech.com/support/DownloadSRDetail_New.aspx?SR_ID=1-MS9MJV&Doc_Source=Download

Detalle:

Las vulnerabilidades identificadas de severidad crítica son:

- Autorización incorrecta: Una aplicación TFTP tiene cargas de archivos sin restricciones a la aplicación web sin autorización, lo cual puede permitir a un atacante ejecutar código arbitrario. Se ha asignado el identificador CVE-2018-7505 para esta vulnerabilidad.
- Gestión incorrecta de rutas de ficheros: Se ha identificado una vulnerabilidad de gestión incorrecta de rutas de ficheros, la cual puede permitir a un atacante ejecutar código arbitrario. Se ha asignado el identificador CVE-2018-10589 para esta vulnerabilidad.
- Desbordamiento de búfer: Se han identificado varias vulnerabilidades de desbordamiento de búfer basadas en pila, que permiten a un atacante ejecutar código arbitrario. Se ha asignado el identificador CVE-2018-7499 para esta vulnerabilidad.
- Desbordamiento de búfer: Se han identificado varias vulnerabilidades de desbordamiento de búfer basadas en pila, que permiten a un atacante ejecutar código arbitrario. Se ha asignado el identificador CVE-2018-8845 para esta vulnerabilidad.
- Puntero no confiable desreferenciado: Se han identificado varias vulnerabilidades de punteros no confiables desreferenciados, lo cual puede permitir a un atacante ejecutar código arbitrario. Se ha asignado el identificador CVE-2018-7497 para esta vulnerabilidad.

Los códigos reservados para el resto de vulnerabilidades de severidad alta y media son: CVE-2018-10590, CVE-2018-7503, CVE-2018-7495, CVE-2018-884, CVE-2018-7501 y CVE-2018-10591

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en puertas de enlace de ABB

Fecha de publicación: 16/05/2018

Importancia: Crítica

Recursos afectados:

- IP-Gateway ? ABB Welcome System Device, versión 3,39 y anteriores
- IP-Gateway - Busch-Jaeger Systemgerät, versión 3,39 y anteriores

Descripción:

El investigador Florian Grunow de ERNW, junto con el apoyo del ICS-CERT, ha reportado estas vulnerabilidades al fabricante ABB. Un atacante que logre explotar estas vulnerabilidades, podría obtener el control remoto del dispositivo y ejecutar código arbitrario.

Solución:

ABB aconseja a sus clientes actualizar los productos con las actualizaciones que han publicado (versión 3.48 y posteriores) para solventar las vulnerabilidades. Se encuentra disponible en el siguiente enlace http://www.busch-jaeger-catalogue.com/software.php

Detalle:

- Inyección de código remoto: Un atacante podría explotar esta vulnerabilidad que afecta a la configuración local de la puerta de enlace vía web. Gracias al envío de paquetes especialmente diseñados, el atacante podría obtener el control del producto y ejecutar código arbitrario. En este caso, el atacante ha de tener acceso directo a la red que permite el acceso vía web a la configuración del dispositivo para explotar la vulnerabilidad. Se ha asignado el código CVE-2017-7931 para esta vulnerabilidad.
- Robo de cookies de sesión: La contraseña de administración se almacena en texto plano mediante una cookie tras un inicio de sesión válido. Un atacante podría aprovecharse de este hecho para extraer la cookie del navegador de una víctima robando así su sesión. Para la explotación de esta vulnerabilidad, el atacante primero ha de comprometer el sistema del cliente. Se ha asignado el código CVE-2017-7906 para esta vulnerabilidad.

Etiquetas: Actualización, Navegador, Vulnerabilidad

Múltiples vulnerabilidades en Switch FL de Phoenix Contact

Fecha de publicación: 17/05/2018

Importancia: Crítica

Recursos afectados:

- Switches FL modelos 3xxx, 4xxx, 48xx con versión de firmware desde la 1.0 a la 1.33.

Descripción:

Los investigadores Vyacheslav Moskvin, Semen Sokolov, Evgeniy Druzhinin, Georgy Zaytsev y Ilya Karpov de Positive Technologies han identificado varias vulnerabilidades de tipo desbordamiento de búfer, exposición de información y ejecución de comandos que afectan a los switches gestionados FL de Phoenix Contact. Un potencial atacante remoto podría conseguir una denegación de servicio, realizar una inyección de comandos o conseguir acceso a información sensible aprovechándose de estas vulnerabilidades.

Solución:

Se recomienda actualizar el firmware a la versión 1.34 o superior mediante la que se solucionan estas vulnerabilidades.

Phoenix Contact también recomienda deshabilitar el agente Web de los switches en las versiones afectadas como medida temporal.

Detalle:

- Un atacante con permisos para transferir ficheros de configuración hacia los dispositivos afectados o permisos para actualizar firmware, podría aprovechar una vulnerabilidad en la comprobación de peticiones en los ficheros CGI ?config_transfer.cgi? y ? software_update.cgi? para ejecutar comandos del sistema operativo y conseguir una denegación de servicio en la red. Se ha reservado el código CVE-2018-10730 para esta vulnerabilidad de severidad crítica.
- Un atacante podría enviar una ?cookie? especialmente diseñada para provocar un desbordamiento de búfer, permitiendo un acceso no autorizado a los ficheros del sistema operativo y la inserción de ficheros con posibilidad de ejecución de código remoto, comprometiendo la integridad del dispositivo. Se ha reservado el código CVE-2018-107228 para esta vulnerabilidad de severidad alta.
- Un atacante podría enviar peticiones GET especialmente diseñadas, aprovechándose el campo cookie, a ?menú_pxc.cgi? o ? index.cgi? para provocar un desbordamiento de búfer y causar una denegación de servicio deshabilitando los servicios Web o Telnet, o ejecutar código de forma remota. Se ha reservado el código CVE-2018-10731 para esta vulnerabilidad de severidad alta.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Inclusión de archivos locales en Ellipse v8 de ABB

Fecha de publicación: 18/05/2018

Importancia: Alta

Recursos afectados:

- Ellipse versiones de la 8.3 a la 8.9

Descripción:

ABB ha recibido información sobre una vulnerabilidad que afecta a la aplicación Ellipse. Se trata de una vulnerabilidad existente en una función RSS con la que un atacante podría acceder a los ficheros almacenados en el sistema de archivos local de forma remota.

Solución:

ABB ha desarrollado unas actualizaciones que corrigen esta vulnerabilidad y recomienda actualizar lo antes posible las versiones vulnerables de la aplicación Ellipse a una versión que solucione los problemas de seguridad.

Detalle:

- La aplicación Ellipse en sus versiones afectadas, contiene funcionalidades que permiten a los usuarios configurar fuentes RSS mediante el uso de URLs vÃ¡lidas. Al utilizar una URL que apunte al sistema de archivos local, un potencial atacante podría ser capaz de obtener acceso a datos confidenciales. Esta acción se debe a una incorrecta validación en los datos de entrada por parte de los usuarios de la aplicación.

Etiquetas: Actualización, Navegador, Vulnerabilidad

Ausencia de cifrado de datos sensibles en N? Vision Clinician Programmer de Medtronic

Fecha de publicación: 18/05/2018

Importancia: Baja

Recursos afectados:

- 8840 N?Vision Clinician Programmer todas las versiones.
- 8870 N?Vision removable Application Card todas las versiones.

Descripción:

Billy Rios de Whitescope LLC ha reportado esta vulnerabilidad al NCCIC que podría permitir el acceso a datos sensibles.

Solución:

Medtronic no ha desarrollado ninguna actualización que solucione esta vulnerabilidad, pero recomienda a los usuarios tomar medidas de seguridad adicionales para minimizar el riesgo de explotar esta vulnerabilidad. Las clínicas y hospitales deberían:

- Mantener un estricto control físico de las tarjetas de aplicación 8870.
- Utilizar únicamente las tarjetas 8870 obtenidas legítimamente y no las proporcionadas por terceros, ya que Medtronic proporciona actualizaciones de firmware y de sistema utilizando las nuevas tarjetas 8870.
- Los programadores 8840 y las tarjetas 8870 son propiedad de Medtronic y deben devolverse a Medtronic cuando ya no estén en uso. Si esto no es posible, deben desecharse de forma segura.

Detalle:

Los datos almacenados en el producto afectado no estÃ¡n cifrados. Un atacante con acceso físico podría acceder a la siguiente información:

- PII - Información personal de identificación. Una combinación de datos personales que permite la identificación única de un individuo.
- PHI - Información personal de salud. Una combinación de PII y datos relacionados con la salud asociados.

Para esta vulnerabilidad se ha reservado el identificador CVE-2018-8849.

Etiquetas: Actualización, Vulnerabilidad

Validación incorrecta en parámetros de entrada en productos de General Electric

Fecha de publicación: 18/05/2018

Importancia: Alta

Recursos afectados:

- PACSystems RX3i CPE305/310 versión 9.20 y anteriores.
- RX3i CPE330 versión 9.21 y anteriores.
- RX3i CPE 400 versión 9.30 y anteriores.
- PACSystems RSTi-EP CPE 100 todas las versiones.
- PACSystems CPU320/CRU320 y RXi todas las versiones.

Descripción:

Younes Dragoni de Nozomi Networks ha reportado al NCCIC esta vulnerabilidad de tipo validación incorrecta en parÃ¡metros de entrada. La explotación remota de esta vulnerabilidad permitiría a un posible atacante causar un reinicio en el sistema afectado o cambios en el estado del dispositivo. Este hecho provocaría un estado de indisponibilidad del dispositivo afectado.

Solución:

General Electric ha publicado una nueva versión de firmware que mitiga esta vulnerabilidad.

- IC695CPE305 - https://digitalsupport.ge.com/communities/en_US/Download/IC695CPE305-PACSystems-RX3i-CPU-DN
- IC695CPE310 ? https://digitalsupport.ge.com/communities/en_US/Download/IC695CPE310-PACSystems-RX3i-CPU-DN
- IC695CPE330 ? https://digitalsupport.ge.com/communities/en_US/Download/IC695CPE330-PACSystems-RX3i-CPU-DN
- IC695CPE400 ? https://digitalsupport.ge.com/communities/en_US/Download/IC695CPE400-PACSystems-RX3i-Rackless-CPU-with-Field-Agent
- CPE100 - https://digitalsupport.ge.com/communities/cc_login?startURL=/en_US/Download/EPSCPE100-RSTi-EP-CPU-Firmware
- CPU/CRU320 ? General Electric ha señalado que este modelo de dispositivo estÃi en el final de su vida útil y por ello recomienda cambiarlo por un modelo mÃis actual.

Detalle:

- Validación incorrecta en parÃimetros de entrada. Esta vulnerabilidad permitiría a un posible atacante causar un estado de indisponibilidad en el dispositivo afectado gracias al envío de peticiones con paquetes especialmente diseñados. Para esta vulnerabilidad se ha reservado el identificador CVE-2018-8867.

Etiquetas: Actualización, Vulnerabilidad

Desbordamiento de búfer en Industrial Automation TPEditor de Delta Electronics

Fecha de publicación: 18/05/2018

Importancia: Alta

Recursos afectados:

- Delta Industrial Automation TPEditor, versiones 1.89 y anteriores.

Descripción:

EL investigador conocido como ThePotato, en colaboración con Trend Micro?s Zero Day Initiative (ZDI), ha identificado una vulnerabilidad de tipo desbordamiento de búfer en el software de programación Industrial Automation TPEditor de Delta Electronics. Un potencial atacante podría causar un desbordamiento de búfer, lo que le permitiría ejecutar código de forma remota.

Solución:

Delta Electronics estÃi trabajando en una nueva versión para corregir esta vulnerabilidad, mientras tanto, recomienda restringir los accesos y emplear solamente ficheros verificados.

Detalle:

Una incorrecta gestión de los ficheros del programa Industrial Automation TPEditor, puede provocar un desbordamiento de búfer. Un atacante con acceso podría explotar esta condición con un fichero especialmente diseñado, lo que le permitiría ejecutar código de forma remota. Se ha reservado el código CVE-2018-8871 para esta vulnerabilidad.

Etiquetas: 0day, Vulnerabilidad

ContraseÃ±as embebidas en controladores STARDOM de Yokogawa

Fecha de publicación: 21/05/2018

Importancia: Crítica

Recursos afectados:

Controladores STARDOM:

- FCJ versión R4.02 o anteriores.
- FCN-100 versión R4.02 o anteriores.
- FCN-RTU versión R4.02 o anteriores.
- FCN-500 versión R4.02 o anteriores.

Descripción:

Yokogawa ha publicado una vulnerabilidad de contraseñas embebidas en los controladores STARDOM. Un potencial atacante podría llegar a ejecutar comandos del sistema.

Solución:

Yokowaga aconseja actualizar a la versión R4.10 o posterior para solucionar esta vulnerabilidad.

Detalle:

Los productos afectados tienen embebidos el usuario y contraseña. Hay un riesgo de que un potencial atacante pueda iniciar sesión en el controlador con la cuenta embebida y pueda ejecutar comandos del sistema.

Etiquetas: Actualización, Vulnerabilidad

Credenciales embebidas en myPRO 7 de mySCADA

Fecha de publicación: 22/05/2018

Importancia: Crítica

Recursos afectados:

- myPRO 7

Descripción:

El investigador de ciberseguridad Emre Ã–VÃœNÃ‡ ha identificado una vulnerabilidad de credenciales embebidas en el software HMI/SCADA myPRO 7 de mySCADA. Un potencial atacante podría utilizar estas credenciales para conectarse al servicio FTP y subir o descargar ficheros.

Solución:

No existe un parche o actualización que solucione esta vulnerabilidad. La única solución posible en este momento consiste en restringir el trÃifico al puerto 2121.

Detalle:

La última versión de myPRO (v7), dispone la información del usuario y contraseña del servidor ftp en el puerto 2121 embebida en un archivo. Un potencial atacante podría utilizar dichas credenciales para cargar o descargar archivos en el servidor que ejecuta el software myPRO. Se ha reservado el identificador CVE-2018-11311 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Vulnerabilidad

Omisión de aviso de acciones inseguras en sistemas BD Kiestra y InoqulA de Becton, Dickinson and Company (BD)

Fecha de publicación: 23/05/2018

Importancia: Media

Recursos afectados:

Los siguientes sistemas utilizan aplicaciones afectadas por las vulnerabilidades:

- BD Kiestra TLA
- BD Kiestra WCA
- Procesador de muestras BD InoqulA

Las aplicaciones afectadas por las vulnerabilidades son:

- Database (DB) Manager, versión 3.0.1.0
- ReadA Overview, versión 1.1.0.2 y anteriores
- PerformA, versión 3.0.0.0 y anteriores

Descripción:

BD ha identificado dos vulnerabilides de no advertencia de acciones no seguras en sistemas que afectan a los sistemas BD Kiestra y InoquIA. Un potencial atacante podría hacer que se perdieran o borraran datos.

Solución:

BD tiene la intención de implementar las mitigaciones necesarias antes de julio de 2018. Esta mitigación incluirÃi la eliminación de la funcionalidad para activar las funciones SQL en DB Manager, PerformA y ReadA. Hasta que esto tenga lugar, BD recomienda los siguientes controles para reducir el riesgo asociado con estas vulnerabilidades:

- DB Manager:
  - El personal de BD Kiestra Laboratory no debe utilizar las funciones SQL asociadas a la funcionalidad en los tres sistemas BD Kiestra: BD Kiestra TLA, BD Kiestra WCA y del procesador de muestras BD InoqulA . Se recomienda no reutilizar los programas actuales a través de la función exportar-importar, sino configurar un nuevo programa o usar las plantillas de programa predefinidas.
  - Asegurarse de que solo el personal autorizado y cualificado tenga derechos de control de acceso a todas las funciones en el DB Manager. Esto se puede configurar a través de la función 'Usuarios' en DB Manager.
- ReadA Overview: se recomienda a los usuarios que configuren la función 'Users' para todos los usuarios en 'none' para acceder a ReadA Overview, si la aplicación no se usa o no se usa habitualmente. Esto se puede configurar a través de la función 'Users' en DB Manager. Si es necesario el uso de ReadA Overview, se recomienda a los usuarios que se aseguren de que solo el personal autorizado y cualificado tengan derechos de control de acceso a todas las funciones en ReadA Overview. Esto se puede configurar a través de la función 'Users' en DB Manager.
- PerformA: se recomienda a los usuarios que garanticen el acceso a los servidores de BD Kiestra para su monitorización mientras se implementan las mejores prÃicticas de seguridad para evitar de manera efectiva el acceso no autorizado a los sistemas BD Kiestra.

Detalle:

Una vulnerabilidad en DB Manager y PerformA y en ReadA permitiría a un usuario autorizado con accesos elevados en el sistema BD Kiestra, usar comandos SQL que pueden resultan en una corrupción de datos. Se han reservado los identificadores CVE-2018-10593 y CVE-2018-10595 para estas vulnerabilidades.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en PlantStruxure PES y

SoMachine Basic de Schneider Electric

Fecha de publicación: 24/05/2018

Importancia: Crítica

Recursos afectados:

- PlantStruxure PES V4.3 SP1 y versiones anteriores
- SoMachine Basic v1.6 SP1 y versiones anteriores

Descripción:

El investigador de ciberseguridad Gjoko Krstikj de Applied y Schneider Electric han identificado varias vulnerabilidades que afectan al software Flexera FlexNet Publisher, usado en el gestor de licencias de PlantStruxure PES y a SoMachine Basic. Un potencial atacante podría aprovechar alguna de estas vulnerabilidades y conseguir la ejecución de comandos, redirigir a los usuarios legítimos a otras pÃiginas o hacer denegaciones de servicio.

Solución:

- Schneider Electric ha desarrollado una la versión 2.1.0.0 del gestor de licencias que soluciona las vulnerabilidades que afectan a PlantStruxure PES. Puede obtenerse en el siguiente enlace: https://www.pes.schneider-electric.com/software-downloads/software/895-floating-license-manager-v2-1-0-0?acm=9_47
- Schneider Electric ha puesto a disposición de los usuarios una actualización para solucionar la vulnerabilidad de SoMachine Basic en el siguiente enlace: https://www.schneider-electric.com/en/download/document/SoMachineBasicV1.6SP1/

Detalle:

- **Desbordamiento de búfer:** OpenSSL 1.0.2h utiliza incorrectamente las comprobaciones de límites de almacenamiento, lo que podría permitir a un potencial atacante remoto causar una denegación del servicio (desbordamiento de entero y bloqueo de la aplicación). Se ha asignado el identificador CVE- 2016-2177 para esta vulnerabilidad de severidad crítica.
- **Desbordamiento de búfer:** El servicio FlexNet Publisher Licensing puede ser explotado para causar una lectura fuera de los límites de la memoria, lo que permitiría a un potencial atacante ejecutar código arbitrario con permisos SYSTEM. Se ha asignado el identificador CVE-2016-10395 para esta vulnerabilidad de severidad alta.
- **Redirección abierta:** El componente lmadmin de Flexera FlexNet Publisher 11.14.1 y anteriores podría permitir a un potencial atacante redirigir a los usuarios a sitios web arbitrarios y llevar a cabo ataques de phising mediante vectores no especificados. Se ha asignado el identificador CVE- 2017-5571 para esta vulnerabilidad de severidad media.
- **Entidad Externa XML (XXE):** Utilizando la técnica de entidades de parÃimetros DTD, un potencial atacante podría conseguir la divulgación y recuperación de datos arbitrarios en el nodo afectado a través del ataque fuera de banda (OOB). La vulnerabilidad se desencadena cuando la información que se pasa al analizador xml no se normaliza al analizar el archivo xml del proyecto/plantilla. Se ha asignado el identificador CVE-2018-7783 para esta vulnerabilidad de severidad alta.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Múltiples vulnerabilidades en TotalAlert Scroll Medical Air Systems de BeaconMedaes

Fecha de publicación: 25/05/2018

Importancia: Alta

Recursos afectados:

- TotalAlert Scroll Medical Air Systems con software versión 4107600010.23 y anteriores.

Descripción:

El investigador Maxim Rupp ha identificado varias vulnerabilidades que afectan al recurso médico TotalAlert Scroll Medical Air Systems de BeaconMedaes. Un potencial atacante podría ver y modificar información del dispositivo y de la configuración de la aplicación web, aunque no tendría acceso a la información médica del usuario. BeaconMedaes informa que un ataque exitoso no afectaría al modo de funcionamiento designado en su propósito.

Solución:

BeaconMedaes ha desarrollado la versión 4107600010.24 y aconseja a todos los usuarios que actualicen sus equipos a la última versión.

Detalle:

- Incorrecta protección de credenciales: Un potencial atacante con acceso de red al servidor web integrado podría recuperar las credenciales definidas por defecto o de un usuario, almacenadas y transmitidas de manera insegura. Se ha reservado el identificador CVE-2018-7518 para esta vulnerabilidad de severidad alta.
- Credenciales almacenadas sin protección: Las contraseñas son almacenadas en texto en claro en un fichero que es accesible sin autenticación. Se ha reservado el identificador CVE-2018-7515 para esta vulnerabilidad de severidad alta.
- Control de acceso inadecuado: Un potencial atacante podría acceder a una URL específica en el servidor web y obtener información en la aplicación sin autenticarse. Se ha reservado el identificador CVE-2018-7526 para esta vulnerabilidad de severidad media.

Etiquetas: Actualización, Vulnerabilidad