Boletín de Abril de 2018

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en productos Building Technologies de Siemens

Fecha de publicación: 02/04/2018

Importancia: Crítica

Recursos afectados:

- License Management System (LMS) todas las versiones anteriores a la V2.1 SP3 (2.1.670).
- Annual Shading V1.0.4 y V1.1.
- Desigo ABT MP1.1 Build 845, MP1.15 Build 360, MP1.16 Build 055, MP1.2 Build 850, MP1.2.1 Build 318, and MP2.1 Build 965.
- Desigo CC MP1.1, MP2.0, MP2.1, y MP3.0.
- Desigo Configuration Manager (DCM) V6.10.140.
- Desigo XWP V5.00.204, V5.00.260, V5.10.142, V5.10.212, V6.00.184, V6.00.342, y V6.10.172.
- SiteIQ Analytics V1.1, V1.2, y V1.3.
- Siveillance Identity V1.1.

Descripción:

Siemens ha publicado un boletín de seguridad con 8 vulnerabilidades, 4 de ellas catalogadas como críticas y 3 altas, que podrían permitir a un atacante ejecutar código arbitrario en los dispositivos afectados o causar una denegación de servicio.

Solución:

Siemens aconseja a los usuarios actualizar las versiones de los productos afectados, para ello recomienda ponerse en contacto con su representante local o con su servicio de atención al cliente:

- Instalar LMS V2.1 SP4 (2.1.681) o superior.

Detalle:

- Vulnerabilidad de severidad crítica provocada por peticiones ASN1 malformadas que podrían causar un desbordamiento de búfer basado en la pila y permitir la ejecución de código arbitrario. Para esta vulnerabilidad se ha reservado el identificador CVE-2017-11496.
- Vulnerabilidad de severidad crítica provocada por nombres de archivo malformados en el paquete de idiomas que podrían causar un desbordamiento de búfer basado en la pila y permitir la ejecución de código arbitrario. Para esta vulnerabilidad se ha reservado el identificador CVE-2017-11497.
- Vulnerabilidad de severidad crítica que puede causar ataques NTLM-relay por medio de la manipulación remota del paquete de idioma. Para esta vulnerabilidad se ha reservado el identificador CVE-2017-12819.
- Vulnerabilidad de severidad crítica causada por una corrupción de memoria puede permitir la ejecución remota de código. Para esta vulnerabilidad se ha reservado el identificador CVE-2017-12821.
- Vulnerabilidad de severidad alta provocada por los archivos HTML de los paquetes de idioma comprimidos pueden permitir el acceso al puntero NULL causando una denegación de servicio remota. Para esta vulnerabilidad se ha reservado el identificador CVE-2017-11498.
- Vulnerabilidad de severidad alta provocada por un desbordamiento de búfer basado en la pila en el analizador XML puede causar una denegación de servicio remota. Para esta vulnerabilidad se ha reservado el identificador CVE-2017-12818.
- Vulnerabilidad de severidad alta provocada por la lectura de memoria arbitraria desde el puntero podría causar una denegación de servicio remota. Para esta vulnerabilidad se ha reservado el identificador CVE-2017-12820.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Denegación de servicio en PLCs WAGO

Fecha de publicación: 02/04/2018

Importancia: Media

Recursos afectados:

Los siguientes versiones de productos de la serie 750 de PLCs WAGO con firmware versión 10 o anterior, están afectados:

- 750-880
- 750-881
- 750-852
- 750-882
- 750-885
- 750-831
- 750-889
- 750-829

Descripción:

Se ha publicado una vulnerabilidad que podría permitir que un atacante provocara una condición de denegación de servicio en los productos afectados.

Solución:

WAGO ha publicado nuevas versiones de firmware que solucionan la vulnerabilidad descrita en este aviso. Para poder obtener las nuevas versiones de firmware, deberá ponerse en contacto con WAGO en el siguiente buzón de correo electrónico: .

Detalle:

Debido a una incorrecta implementación de la negociación inicial en tres fases propio de una comunicación TCP, un atacante remoto, podría afectar a las comunicaciones con las herramientas de comisión y servicio. Igualmente, mediante el envío de paquetes especialmente diseñados al puerto 2455 TCP/IP (usado por el software de gestión Codesys), podría provocarse una condición de denegación de servicio en las comunicaciones con las citadas herramientas de comisión y servicio.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en dispositivos MicroLogix 1400

Fecha de publicación: 02/04/2018

Importancia: Crítica

Recursos afectados:

- Allen-Bradley Micrologix 1400 Series B FRN 21.003
- Allen-Bradley Micrologix 1400 Series B FRN 21.002
- Allen-Bradley Micrologix 1400 Series B FRN 21.0
- Allen-Bradley Micrologix 1400 Series B FRN 15

Descripción:

Los investigadores Jared Rittle y Patrick DeSantis, de Cisco Talos, han reportado múltiples vulnerabilidades que afectan a productos de Rockwell y que podrían causar la denegación del servicio,la divulgación de información confidencial, la pérdida de comunicación y/o la modificación de la configuración o la escala lógica.

Solución:

Se recomienda actualizar el firmware de los dispositivos afectados a la versión:

- Allen-Bradley Micrologix 1400 FRN 21.004

Para usuarios de Micrologix 1400 Serie A o para usuarios de Micrologix 1100 se recomienda migrar a Micrologix 1400 Serie B o C y para esto Rockwell Automation recomienda que se pongan en contacto con su distribuidor. Puede encontrar más información en la página de Rockwell Automation sobre esta vulnerabilidad.

Además se recomienda a los usuarios afectados establecer el valor de la clave ?keyswitch? al valor ?Hard Run? para evitar cualquier cambio no autorizado.

Cisco Talos también ha generado reglas de seguridad para SNORT para detectar posibles ataques que utilicen estas vulnerabilidades, con los siguientes identificadores (SID): 44424, 44425, 44426, 44427, 44428 y 44429

Detalle:

Las vulnerabilidades detectadas por los investigadores de Cisco Talos son las siguientes:

- Vulnerabilidad de denegación de servicio por un paquete malformado de la tarjeta Ethernet: esta vulnerabilidad permitiría a un atacante alterar el ciclo de potencia del dispositivo y causar un fallo del mismo, para aprocecharse de esta vulnerabilidad además no es necesario utilizar Ethernet/IP por lo que deshabilitarlo usando RSLogix no sería suficiente. Se ha asignado el identificador CVE-2017-12088 para esta vulnerabilidad.
- Vulnerabilidad de denegación de servicio mediante la funcionalidad de descarga: Un atacante remoto no autenticado podría enviar un paquete especialmente diseñado al controlador durante el proceso de descarga estándar. Sin el paquete adecuado para indicar la finalización de la descarga, el controlador. Se ha asignado el identificador CVE-2017-12089 para esta vulnerabilidad.
- Vulnerabilidad de denegación de servicio con una solicitud de establecimiento de SNMP: Una solicitud de configuración de SNMP especialmente diseñada, cuando se envía sin los valores adecuados para cambiar parámetros del firmware podría causar que el dispositivo se apague y cause la denegación de servicio. Se ha asignado el identificador CVE-2017-12090 para esta vulnerabilidad.
- Vulnerabilidad en el control de acceso al dispositivo: Un atacante remoto no autenticado podría enviar un paquete especialmente diseñado al dispositivo afectado y utilizar operaciones de lectura o escritura que podrían generar varios impactos potenciales, que van desde la divulgación de información confidencial, la modificación de configuraciones o la modificación de la lógica del programa. Se han asignado los identificadores CVE-2017-14462 a CVE-2017-14473 para esta vulnerabilidad en función del parámetro o fichero afectado.
- Vulnerabilidad de escritura de archivos en el módulo de memoria: El módulo de memoria instalado en un controlador MicroLogix que permite al usuario instruir al controlador para que escriba su programa en el módulo sin autenticación. El módulo de memoria

es una copia de seguridad, pero también se puede usar para cargar programas una vez que se produce un error, y tiene la capacidad de cargar el programa cada vez que se enciende el dispositivo. Se ha asignado el identificador CVE-2017-12092 para esta vulnerabilidad.
- Vulnerabilidad de registro de sesión maliciosa o pérdida de las comunicaciones: El controlador MicroLogix 1400 admite diez sesiones activas a la vez. La vulnerabilidad descubierta consiste en que un usuario malintencionado puede enviar sus propios paquetes de sesión para crear su propia conexión con el controlador, evitando que los usuarios válidos accedan al PLC. Además cuando ya hay diez conexiones, al enviar una nueva la más antigua se desconecta provocando el corte de la comunicación. Se ha asignado el identificador CVE-2017-12093 para esta vulnerabilidad.

Etiquetas: Actualización, SCADA, Vulnerabilidad

Vulnerabilidad en AWK-3131A de Moxa

Fecha de publicación: 04/04/2018

Importancia: Crítica

Recursos afectados:

- Moxa AWK-3131A Industrial IEEE 802.11a/b/g/n wireless AP/bridge/client versión 1.7 y anteriores.

Descripción:

Los investigadores Patrick DeSantis y Dave McDaniel de Cisco Talos han detectado una vulnerabilidad de severidad crítica en los dispositivos de red inalámbrica industrial AWK-3131A de Moxa. Esta vulnerabilidad podría permitir a un atacante remoto y sin autenticación adquirir privilegios de administración y ejecución de comandos en el sistema operativo.

Solución:

El fabricante Moxa ha puesto a disposición de los usuario una actualización de firmware que soluciona la vulnerabilidad. Esta actualización esta disponible a través del siguiente enlace:

- Firmware para AWK-3131A versión 1.10

Detalle:

La vulnerabilidad detectada es debida a una mala gestión de los inicios de sesión fallidos, permitiendo a un usuario remoto sin autenticación inyectar código a través del campo de inicio de sesión de diferentes servicios (SSH, Telnet, consola de comandos). Esto podría permitir al atacante ejecutar comandos en el sistema operativo con privilegios de administración. Se ha reservado el identificador CVE-2017-14459 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Acceso a la clave privada del servidor web de Moxa MXview

Fecha de publicación: 06/04/2018

Importancia: Alta

Recursos afectados:

- MXview versiones 2.8 y anteriores

Descripción:

El investigador Michael DePlante del Centro Leahy para Investigación Digital informó de una vulnerabilidad en el servidor web de Moxa MXview que permitiría a un atacante remoto acceder y leer las claves privadas criptográficas del servidor.

Solución:

- Moxa ha publicado en su web la versión 2.9 de MXView que corrige esta vulnerabilidad.

Detalle:

La vulnerabilidad detectada podría permitir leer y acceder a la clave privada del servidor web a través de una petición HTTP GET, permitiendo al atacante remoto descifrar la información trasmitida al servidor web. Se ha asignado el identificador CVE-2018-7506 a esta vulnerabilidad.

Etiquetas: Actualización, SCADA

Múltiples vulnerabilidades en U.motion Builder de Schneider Electric

Fecha de publicación: 09/04/2018

Importancia: Crítica

Recursos afectados:

- U.motion Builder Software, versiones 1.3.4 y anteriores

Descripción:

Los investigadores Rgod de Zero-Day Initiative y Constantin-Cosmin Craciun han identificado múltiples vulnerabilidades que afectan al software U.motion Builder de Schneider Electric. Un potencial atacante podría realizar ejecución remota de código revelación no autorizada de datos.

Solución:

Schneider Electric ha publicado un parche que soluciona estas vulnerabilides. El parche puede obtenerse en:

https://www.schneider-electric.com/en/download/document/SE_UMOTION_BUILDER/

Schneider Electric también recomienda seguir las siguientes medidas preventivas de seguridad y buenas prácticas:

- Disponer de un cortafuegos delante de la máquina que ejecuta U.motion Builder, con reglas de control de acceso restrictivas.
- No se debe conectar esa máquina directamente a Internet.
- No se debe ubicar esta máquina en una DMZ.
- No se debe permitir el tráfico directamente desde Internet hacia la máquina.
- El acceso remoto contra U.motion System dentro de esta máquina debe realizarse siempre bajo una conexión VPN segura.
- Limitar las conexiones a U.motion Builder software solamente a máquinas de confianza con una necesidad real.
- Usar listas blancas para limitar quien puede ejecutar esta aplicación U.builder Software dentro de la propia máquina.
- Utilizar los controles de acceso que proporciona de manera nativa el propio cortafuegos de Windows.

Detalle:

A continuación se detallan las vulnerabilidades de severidad alta o crítica:

- Inyección SQL que permite ejecución remota de código: El parámetro de entrada ?object_id? es susceptible de inyección SQL dentro del fichero track_getdata.php. Esta vulnerabilidad podría permitir a un potencial atacante la ejecución de código arbitrario. Se ha asignado el identificador CVE-2018-7765 para esta vulnerabilidad de severidad alta.
- Ejecución de código remoto: El parámetro ?update_file? en el fichero update_module.php no posee un manejo adecuado. Un atacante remoto autenticado podría explotar esta vulnerabilidad gracias al envío de peticiones especialmente elaboradas al servidor. Se ha asignado el identificador CVE-2018-7777 para esta vulnerabilidad de severidad alta.
- Samba Cry: Clientes maliciosos pueden subir una librería a la carpeta compartida del servidor smbd con permisos de escritura y hacer que éste las ejecute. Se ha asignado el identificador CVE-2017-7494 para esta vulnerabilidad de severidad crítica.

Los códigos reservados para el resto de vulnerabilidades de critidad media son: CVE-2018-7763, CVE-2018-7764, CVE-2018-7766, CVE-2018-7767, CVE-2018-7768, CVE-2018-7769, CVE-2018-7770, CVE-2018-7771, CVE-2018-7772, CVE-2018-7773, CVE-2018-7774, CVE-2018-7775, CVE-2018-7776 .

Etiquetas: Actualización, PHP, Schneider Electric, Vulnerabilidad

---

Múltiples vulnerabilidades en software CX-One de Omron

Fecha de publicación: 11/04/2018

Importancia: Media

Recursos afectados:

- CX-One version 4.42 y anteriores, incluyendo las siguientes aplicaciones:
  - CX-FLnet versión 1.00 y anteriores
  - CX-Protocol versión 1.992 y anteriores
  - CX-Programmer versión 9.65 y anteriores
  - CX-Server versión 5.0.22 y anteriores
  - Network Configurator versión 3.63 y anteriores
  - Switch Box Utility versión 1.68 y anteriores

Descripción:

El investigador Rgod de Zero Day Initiative de Trend Micro ha descubierto dos vulnerabilidades de desbordamiento de búfer y una de acceso a recursos con un tipo incompatible que afectan al software CX-One de Omron. Un potencial atacante podría conseguir una ejecución remota de código.

Solución:

Omron ha publicado nuevas versiones de los productos afectados, en concreto ha publicado:

- X-FLnet versión 1.10,
- CX-Protocol versión 1.993,
- CX-Programmer versión 9.66,
- Common Module que incluye CX-Server versión 5.0.23,
- Network Configurator versión 3.64, and
- Switch Box Utility versión 1.69

Detalle:

- Desbordamiento de pila: El tratamiento de ficheros de proyecto malformados puede provocar un desbordamiento de búfer que afecte tanto a la stack como a la heap. Se han asignado los códigos CVE-2018-8834 y CVE-2018-7514 para esta vulnerabilidad.
- Acceso a recursos con un tipo incompatible: El tratamiento de ficheros de proyecto malformados podría permitir al puntero llamar a un objeto incorrecto resultado en el acceso a un recurso usando una condición de tipo incompatible. Se ha asignado el código CVE-2018-7530 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en sistemas de notificación masiva de emergencias de ATI Systems

Fecha de publicación: 11/04/2018

Importancia: Media

Recursos afectados:

- HPSS16
- HPSS32
- MHPSS
- ALERT4000

Descripción:

Balint Seeber de Bastille ha reportado una vulnerabilidad de autenticación inadecuada y otra de falta de cifrado que afectan a diferentes dispositivos de notificación masiva de emergencias de ATI Systems. Un potencial atacante podría provocar falsas alarmas.

Solución:

ATI Systems ha creado un parche que añade nuevas funcionalidades de seguridad a los paquetes enviados vía radio. ATI Systems está probando el parche y será distribuido bajo petición, además indica que muchos sistemas están diseñados específicamente para los usuarios y son estos los que deben asegurarse de que las actualizaciones sean apropiadas para sus sistemas.

ATI Systems recomienda que, cuando sea posible los sistemas de radio de voz simple sean sustituidos por sistemas de radio digitales P-25 (APCO), que proporcionan enlaces cifrados seguros.

Detalle:

- Autenticación inadecuada: Un paquete de radio especialmente malformado podría permitir a un potencial atacante lanzar alarmas falsas de forma remota. Se ha reservado el identificador CVE-2018-8862 para esta vulnerabilidad.
- Falta de cifrado de datos sensibles: Un paquete de radio especialmente malformado podría permitir a un potencial atacante lanzar alarmas falsas de forma remota. Se ha reservado el identificador CVE-2018-8864 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Privacidad, Vulnerabilidad

Debilidad en control de acceso en CENTUM y Exaopc de Yokogawa

Fecha de publicación: 13/04/2018

Importancia: Media

Recursos afectados:

- CENTUM series
  - Todas las versiones de CENTUM CS 1000
  - CENTUM CS 3000 versiones R3.09.50 y anteriores
  - CENTUM CS 3000 Small versiones R3.09.50 y anteriores
  - CENTUM VP versiones R6.03.10 y anteriores
  - CENTUM VP Small versiones R6.03.10 y anteriores
  - CENTUM VP Basic versiones R6.03.10 y anteriores
- Exaopc versiones R3.75.00 y anteriores
- Todas las versiones B/M9000 CS
- B/M9000 VP versiones R8.01.01 y anteriores

Descripción:

La empresa Yokogawa en colaboración con JPCERT, han reportado una vulnerabilidad sobre debilidades en permisos, privilegios y control de accesos en CENTUM y Exaopc de Yokogawa. Un potencial atacante podría generar alarmas falsas de proceso o sistema o bloquear el sistema o los procesos de visualización de alarmas.

Solución:

Yokogawa ha publicado una serie de mitigaciones para los productos afectados.

- Serie CENTUM
  - CENTUM CS 1000, CENTUM CS 3000, CENTUM CS 3000 Small: No serán proporcionadas actualizaciones ya que estos dispositivos se encuentran fuera de soporte. El fabricante recomienda cambiar el dispositivo a la última versión de CENTUM VP.
  - CENTUM VP, CENTUM VP Small, CENTUM VP BASIC: Los usuarios afectados pueden actualizar estos dispositivos a la versión R5.04.B2 o R6.04.00.
- Exaopc: los usuarios afectados deberían actualizar el sistema a la versión R3.76.00.
- B/M9000CS: la vulnerabilidad no existe en este producto, sin embargo, la existencia de software al que sí afecta esta vulnerabilidad en el mismo PC puede afectar a las alarmas del dispositivo.
- B/M9000 VP: la vulnerabilidad no existe en este producto, sin embargo, la existencia de software al que sí afecta esta vulnerabilidad en el mismo PC puede afectar a las alarmas del dispositivo.

Detalle:

Una debilidad en el control de acceso podría permitir a un atacante explotar de forma local una función relacionada con la gestión de mensajes en el sistema. Se ha reservado el identificador CVE-2018-8838 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en router industrial EDR-810 de Moxa

Fecha de publicación: 16/04/2018

Importancia: Alta

Recursos afectados:

- Moxa EDR-810 V4.1 build 17030317 y quizás versiones anteriores

Descripción:

El investigador Carlos Pacho de Cisco Talos ha descubierto múltiples vulnerabilidades en el router industrial Moxa EDR-810. Estas vulnerabilidades afectan principalmente al servidor web que posee el dispositivo y entre otras acciones, un atacante podría realizar: una elevación de privilegios mediante inyección de comandos, revelación no autorizada de información (incluyendo contraseñas del dispositivo), cambios en la configuración mediante CSRF o provocar condiciones de denegación de servicio en los productos afectados.

Solución:

El fabricante ha publicado una actualización de firmware que resuelve todas las vulnerabilidades que afectan al dispositivo.

Esta actualización puede descargarse en el siguiente enlace:

https://www.moxa.com/support/download.aspx?type=support&id=15851

Detalle:

A continuación, se detallan las vulnerabilidades con severidad alta:

- Inyección de comandos: un atacante podría enviar una petición POST especialmente diseñada al servidor web del dispositivo para lograr una escalada de privilegios en el sistema. Un atacante podría explotar esta vulnerabilidad inyectando comandos de Sistema Operativo en el parámetro ip de la URI ?*/goform/net_WebPingGetValue*?. Se ha asignado el identificador CVE-2017-12120 para esta vulnerabilidad.
- CSRF: vulnerabilidad (Cross-Site Request Forgery) en una funcionalidad del servidor Web del Moxa EDR-810 V4.1, permitiría a un atacante explotar esta vulnerabilidad CSRF, mediante el envió de un paquete HTTP especialmente diseñado. El atacante se aprovecharía de dicho paquete para realizar acciones que puedan comprometer el dispositivo. Se han asignado el código CVE-2017-12126 para esta vulnerabilidad.
- Inyección de comandos: vulnerabilidad de Inyección de comandos en una de las funcionalidades del servidor Web OpenVPN del Moxa EDR-810 V4.1. Un atacante podría explotar estar vulnerabilidad mediante el envío de un paquete HTTP mediante el método POST especialmente diseñado. Este paquete permitiría al atacante, realizar una escalada de privilegios, obteniendo una "shell" de superusuario con máximos privilegios. Un atacante podría explotar esta vulnerabilidad inyectando comandos de Sistema Operativo en los parámetros de la URI "/goform/net_Web_get_value". Se han asignado los siguientes códigos CVE-2017-14432 y CVE-2017-14434, para esta vulnerabilidad.
- Inyección de comandos: un atacante podría enviar una petición POST especialmente diseñada al servidor web del dispositivo para lograr una escalada de privilegios en el sistema. Esta petición permitiría al atacante, realizar una escalada de privilegios, obteniendo una "shell" de superusuario con máximos privilegios. Un atacante podría explotar esta vulnerabilidad inyectando comandos de Sistema Operativo en el parámetro rsakey_name de la URI ?*/goform/WebRSAKEYGen*?. Se ha asignado el identificador CVE-2017-12121 para esta vulnerabilidad.
- Inyección de comandos: un atacante podría enviar una petición POST especialmente diseñada al servidor web del dispositivo para lograr una escalada de privilegios en el sistema. Esta petición permitiría al atacante, realizar una escalada de privilegios, obteniendo una "shell" de superusuario con máximos privilegios. Un atacante podría explotar esta vulnerabilidad inyectando comandos de Sistema Operativo en el parámetro CN de la URI ?*/goform/net_WebCSRGen*?. Se ha asignado el identificador CVE-2017-12125 para esta vulnerabilidad.
- ?*Service Agent*? con múltiples vulnerabilidades DoS: la funcionalidad ?*Service Agent*? que posee el dispositivo Moxa EDR-810 (V4.1 build 17030317) posee vulnerabilidades DoS. Un paquete especialmente diseñado, enviado al puerto 4000/tcp o al 4001/tcp, podría desencadenar una denegación de servicio. Se han asignado los identificadores CVE-2017-14438 y CVE-2017-14439 para estas vulnerabilidades.
- Validación de datos de entrada incorrecta: una URI HTTP especialmente diseñada, podría causar una vulnerabilidad de desreferencia de puntero NULL que resulte en un fallo en el servidor web. Un potencial atacante podría ocasionar una denegación de servicio mediante el envío de una URI malformada. Se ha reservado el identificador CVE-2017-12124 para esta vulnerabilidad.
- Denegación de Servicio en una de las funcionalidades del servidor Web del Moxa EDR-810 V4.1. Un atacante podría provocar una denegación de servicio mediante el envío de una URI HTTP especialmente malformada. Esta petición provocaría una desreferencia de puntero NULL mal gestionada. El envío de una petición mediante el método GET contra "/MOXA_LOG.ini, /MOXA_CFG.ini, o /MOXA_CFG2.ini" sin la cabecera cookie produciría esta vulnerabilidad. Se han asignado los siguientes códigos CVE-2017-14435 y CVE-2017-14437, para esta vulnerabilidad.

Los códigos reservados para el resto de vulnerabilidades de severidad media y baja son: CVE-2017-12123, CVE-2017-12128, CVE-2017-12127 y CVE-2017-12129.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Schneider Electric

Fecha de publicación: 18/04/2018

Importancia: Crítica

Recursos afectados:

- Triconex Tricon de Schneider Electric, modelo MP 3008 versiones firmware10.0-10.4
- InduSoft Web Studio v8.1 y versiones anteriores
- InTouch Machine Edition 2017 v8.1 y versiones anteriores

Descripción:

Tenable Research reportó una vulnerabilidad a Schneider Electric de tipo desbordamiento de búfer. Además, el NCCIC y Schneider Electric han descubierto otras dos vulnerabilidades adicionales durante la investigación del malware HatMan.

Un atacante que aprovechara estas vulnerabilidades podría realizar entre otras acciones: ejecución arbitraria de código, apagado de sistemas, compromiso de los sistemas de protección o compromiso total de los dispositivos afectados.

Solución:

- En el caso de la vulnerabilidad de desbordamiento de búfer en Indusoft Web Studio e InTouch Machine Edition, el fabricante recomienda actualizar las versiones afectadas de los productos vulnerables:
  - Usuarios que usen InduSoft Web Studio v8.1 o versiones anteriores deberían actualizar a la versión InduSoft Web Studio v8.1 SP1 lo antes posible. A continuación, se proporciona el enlace para descargar la actualización: http://download.indusoft.com/81.1.0/IWS81.1.0.zip
  - Usuarios que usen Machine Edition 2017 v8.1 o versiones anteriores deberían actualizar a la versión Machine Edition 2017 v8.1 SP1 lo antes posible. A continuación, se proporciona el enlace para descargar la actualización: https://fs-ext.invensys.com/adfs/ls/?wa=wsignin1.0&wtrealm=https://gcsresource.schneider-electric.com&wctx=rm=0&id=passive&ru=%2ftracking%2fConfirmDownload.aspx%3fid%3d22530&wct=2018-04-18T07:35:10Z
- En el caso de la vulnerabilidad que afecta al dispositivo Triconex Tricon, el fabricante recomienda actualizar el firmware a su última versión 11.X que resuelve todas las vulnerabilidades que afectan al dispositivo.

Detalle:

A continuación, se detallan las vulnerabilidades que afectan a Triconex Tricon de Schneider Electric, modelo MP 3008:

- **Gestión incorrecta de los permisos de escritura en el espacio de memoria**: Las llamadas de sistema leen directamente del espacio de memoria sin un control por parte del proceso y sin ninguna comprobación. La manipulación de los datos en memoria permitiría a un atacante copiar instrucciones en cualquier espacio la memoria. Se han asignado el código CVE-2018-8872 para esta vulnerabilidad de severidad crítica.

- **Gestión incorrecta de los permisos de escritura en el espacio de memoria**: Cuando se realiza una llamada a sistema, los registros son almacenados en una posición fija. Un atacante puede modificar datos en este espacio de memoria fijo y tomar el control de los estados de los sistemas o del sistema de supervisor. Se han asignado el código CVE-2018-7522 para esta vulnerabilidad de severidad alta.

Por otro lado, el detalle de la vulnerabilidad que afecta a los productos Indusoft Web Studio e InTouch Machine Edition es:

- **Desbordamiento de búfer:** Un atacante remoto podría elaborar un paquete malformado para enviar durante los eventos de lectura o escritura en alarmas, etiquetas o acciones, pudiendo lograr la ejecución de código remoto con máximos privilegios. Se ha reservado el identificador CVE-2018-8840 para esta vulnerabilidad de severidad crítica.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Múltiples vulnerabilidades en implantes cardíacos ICD y CRT-D de Abbott Laboratories

Fecha de publicación: 18/04/2018

Importancia: Alta

Recursos afectados:

Los siguientes modelos de ICD (Implantable Cardioverter Defibrillator) y CRT-D (Cardiac Synchronization Therapy Defibrillator) de Abbott Laboratories:

- Fortify
- Fortify Assura
- Quadra Assura
- Quadra Assura MP
- Unify
- Unify Assura
- Unify Quadra
- Promote Quadra
- Ellipse
- Current
- Promote

Descripción:

MedSec Holdings Ltd. ha reportado estas vulnerabilidades al NCCIC y Abbott Laboratories. Un atacante cercano al dispositivo puede interferir en el rango de radio frecuencia, saltarse la autenticación y acceder sin permiso para cambiar comandos, modificar variables o interferir en el correcto funcionamiento del mismo.

Solución:

El fabricante ha publicado una actualización de firmware que resuelve todas las vulnerabilidades identificadas en sus productos. Esta actualización puede ser aplicada a través de Merlin PCS Programmer por el proveedor de atención médica. Abbott y la FDA recomiendan esta actualización para todos los pacientes en la próxima visita programada o cuando sea apropiado dependiendo de las preferencias del paciente y del médico. Los ICD y CRT-D fabricados a partir del 25 de abril de 2018 ya contarán con estas actualizaciones preinstaladas.

Además, desde el Cybersecurity Medical Advisory Board se recomiendan las siguientes medidas preventivas:

- Los proveedores de atención médica y los pacientes deben analizar los riesgos y beneficios de estas vulnerabilidades y de las actualizaciones del firmware correspondiente durante la próxima visita, teniendo en cuenta los casos concretos de los pacientes, tales como dependencia del marcapasos, la frecuencia de la terapia de alto voltaje, la edad del dispositivo, la preferencia del paciente, también se deberá de proporcionar a los pacientes la "Comunicación con el paciente".
- Determinar si la actualización del firmware es apropiada dado el riesgo de actualización para el paciente. Si se considera apropiado, instalar la actualización de firmware conforme a las instrucciones proporcionadas por el fabricante.
- Las actualizaciones del firmware deben de llevarse a cabo en una instalación que disponga de sistemas adecuados de monitorización y desfibrilación externa.

Detalle:

- Autenticación incorrecta: El algoritmo empleado para la autenticación, que utiliza una clave de autenticación y un valor de tiempo, pueden ser comprometido o evitado, esto permitiría a un atacante cercado enviar comandos a los dispositivos ICD o CRT-D modificando las señales de radio frecuencia. Se han asignado el código CVE-2017-12712 para esta vulnerabilidad de severidad alta.
- Restricciones incorrectas sobre peticiones que afectan al consumo de batería: Los ICD o CRT-D no disponen de una correcta gestión del número de peticiones que se pueden realizar del tipo ?RF wake-up?, esto permitiría a un atacante cercano abusar del envío de este tipo de comandos para reducir el tiempo de vida útil de la batería. Se han asignado el código CVE-2017-12714 para esta vulnerabilidad de severidad media.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en CARTO 3 de Biosense Webster

Fecha de publicación: 18/04/2018

Importancia: Crítica

Recursos afectados:

- Sistemas CARTO 3 fabricados antes de abril del 2018

Descripción:

Las vulnerabilidades que afectan al sistema CARTO 3 podrían permitir a un atacante con acceso físico al dispositivo, acceder a información almacenada en el propio dispositivo, incluyendo información médica de los pacientes, afectando a la integridad del sistema CARTO 3 y podría llegar a generar una situación de denegación de servicio.

Solución:

Biosense Webster está poniéndose en contacto con los clientes afectados para iniciar el proceso de actualización para mitigar las vulnerabilidades.

Desde Biosense Webster recomiendan restringir el acceso físico a cualquier producto de la familia CARTO 3 hasta recibir el parche de seguridad.

Detalle:

Un atacante con acceso físico al sistema CARTO 3 V4 y con conocimiento de las vulnerabilidades, podría explotar alguna de las vulnerabilidades pudiendo llegar a comprometer la información del dispositivo, así como afectar a la integridad y disponibilidad del sistema.

Para más detalles de la lista completa de vulnerabilidades puede consultar el aviso oficial de Biosense Webster.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en Relion 630 series de ABB

Fecha de publicación: 18/04/2018

Importancia: Crítica

Recursos afectados:

- Relion® 630 series 1.1
- Relion® 630 series 1.2
- Relion® 630 series 1.3
- Relion® 630 series 1.1, 1.1.0.C1 y anteriores.
- Relion® 630 series 1.2, 1.2.0.B4 y anteriores.
- Relion® 630 series 1.3, 1.3.0.A7 y anteriores.

Descripción:

Los investigadores Aleksandr Tlyapov (Kaspersky Lab), Kirill Nesterov (Kaspersky Lab), Ilya Karpov, Evgeniy Druzhinin, Damir Zainullin (Positive Technologies) y Victor Nikitin (i-Grids) han descubierto varias vulnerabilidades cuya explotación podría permitir a un atacante realizar las siguientes acciones: borrado/modificación de la base de datos que podría desencadenar en una condición de denegación de servicio del dispositivo, lectura y modificación de cualquier archivo de la memoria flash sin autenticación que podría provocar una condición de denegación de servicio en el dispositivo u otra condición de denegación de servicio en los productos afectados.

Solución:

Existen versiones de firmware que solucionarían las vulnerabilidades descritas en este aviso salvo la de cifrado débil de la base de datos de severidad media.

Consultar los siguientes enlaces para ver qué versiones de firmware solucionan las vulnerabilidades descritas:

http://search.abb.com/library/Download.aspx?DocumentID=1MRS758877&LanguageCode=en&DocumentPartId=&Action=Launch

http://search.abb.com/library/Download.aspx?DocumentID=1MRS758878&LanguageCode=en&DocumentPartId=&Action=Launch

http://search.abb.com/library/Download.aspx?DocumentID=1MRS758909&LanguageCode=en&DocumentPartId=&Action=Launch

Detalle:

A continuación, se detallan las vulnerabilidades que afectan los dispositivos Relion 630 series de ABB:

- Gestión incorrecta de las rutas de los ficheros: Una vulnerabilidad en el servidor de MMS incluido en los dispositivos afectados, permitiría a un atacante enviar peticiones especialmente malformadas, para acceder a rutas de ficheros fuera de los límites del directorio COMTRADE, aprovechándose de los comandos fopen y fdelete. Esto permitiría la lectura/escritura de ficheros en cualquier ruta, saltándose la limitación del directorio especificado para su función. Esta vulnerabilidad solo afectaría a los dispositivos que tengan habilitado el protocolo IEC 61850 MMS.
- Vulnerabilidad en la generación de claves de encriptación de la base de datos: un atacante puede aprovecharse de esta vulnerabilidad para modificar la base de datos, estas modificaciones pueden derivar en una Denegación de Servicio.
- Vulnerabilidad en el manejador de comandos: un atacante puede aprovecharse de esta vulnerabilidad, enviando paquetes malformados que provocarían el reinicio forzoso de este dispositivo. Durante la fase de reinicio, la funcionalidad principal de protección del dispositivo no estaría disponible.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Rockwell Automation

Fecha de publicación: 18/04/2018

Importancia: Crítica

Recursos afectados:

Dispositivos con versiones vulnerables de Cisco IOS o IOX XE:

- Switches Ethernet gestionados Allen-Bradley Stratix 8300 Industrial, versiones 15.2(4a)EA5 y anteriores.
- Switches Allen-Bradley Stratix 5400 Industrial, versiones 15.2(6)E0a y anteriores.
- Switches Allen-Bradley Stratix 5410 Industrial Distribution, versiones 15.2(6)E0a y anteriores
- Switches Ethernet gestionados Allen-Bradley Stratix 5700 Industrial, versiones 15.2(6)E0a y anteriores
- Switches Ethernet gestionados Allen-Bradley Stratix 8000 Modular, versiones 15.2(6)E0a y anteriores
- Switches industriales gestionados para entornos extremos Allen-Bradley ArmorStratix 5700 Industrial, versiones 15.2(6)E0a y anteriores
- Router Allen-Bradley Stratix 5900 Services, versión 15.6.3M1 y anteriores.

Descripción:

Rockwell Automation ha reportado estas vulnerabilidades al NCCIC a través de la publicación semestral de ?*Cisco IOS and IOS XE Software Security Advisory Bundled Publication?*. Un atacante remoto podría aprovechar estos tipos de vulnerabilidades: parámetros de entrada inválidos, gestión incorrecta de errores, incorrecta restricción de operaciones dentro de los límites de la memoria del buffer o formato de cadenas controladas externamente para lograr pérdidas de disponibilidad, confidencialidad y/o integridad causadas por un agotamiento de recursos en la memoria, reinicio de módulos de comunicación, información corrupta y/o exposición de la información.

Solución:

Cisco ha publicado reglas Snort en el siguiente enlace:

https://www.cisco.com/web/software/286271056/117258/sf-rules-2018-03-29-new.html

Estas reglas mitigan las vulnerabilidades asociadas a los siguientes códigos:

- **CVE-2018-0171** ? Regla Snort número 46096 y 46097
- **CVE-2018-0156** ? Regla Snort número 41725
- **CVE-2018-0174** ? Regla Snort número 46120
- **CVE-2018-0172** ? Regla Snort número 46104
- **CVE-2018-0173** ? Regla Snort número 46119
- **CVE-2018-0158** ? Regla Snort número 46110

Cisco añade las siguientes notas asociadas a las vulnerabilidades (**CVE-2018-0171 y CVE-2018-0156**):

- La funcionalidad Smart Install viene desactivada por configuración expresa, sin embargo, la actualización de los switches, que no su reinstalación, podría habilitar esta opción.
- Deshabilitar la funcionalidad Smart Install con el comando de configuración "no vstack "si no es necesario o una vez realizada la instalación.
- Los usuarios que utilicen la funcionalidad Smart Install (y deben dejarla deshabilitada), pueden usar ACLs para bloquear el tráfico entrante en el puerto 4786/tcp.

CVE-2018-0155: Los administradores que no utilicen la funcionalidad BFD en sus entornos pueden desactivar dicha funcionalidad con su correspondiente comando "bfd" para evitar posibles explotaciones de la vulnerabilidad.

Por otro lado, los administradores que utilicen esta funcionalidad, pueden implementar políticas de control (CoPP) para permitir sólo el procesamiento de paquetes BFD conocidos y limitar así la exposición del producto afectado.

Las vulnerabilidades asociadas a los códigos **CVE-2018-0167** y **CVE-2018-0175** no tienen formas de mitigación específicas. Se aconseja visitar el siguiente enlace del fabricante para más información:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-lldp

Por su parte, el fabricante Rockwell Automation recomienda seguir las siguientes medidas preventivas de seguridad y buenas prácticas:

- Ayudar a minimizar la exposición de todos los dispositivos y/o sistemas de control tras cortafuegos y confirmar que los dispositivos y/o sistemas no poseen acceso a Internet.
- Separar las redes de control y los dispositivos industriales de las redes corporativas.

Cuando sea necesario un acceso remoto, utilizar mecanismos de seguridad como Virtual Private Networks (VPNs).

Detalle:

- **Validación de datos de entrada inadecuada**: Una vulnerabilidad en la funcionalidad Smart Install del Software Cisco IOS y Cisco IOS XE podría permitir a un atacante remoto sin autenticación desencadenar un reinicio en un dispositivo afectado, dando como resultado una condición de denegación de servicio (DoS) o la ejecución de código arbitrario en el dispositivo afectado. La vulnerabilidad se debe a una validación incorrecta de los datos del paquete. Un atacante podría explotar esta vulnerabilidad enviando un paquete de mensaje Smart Install a un dispositivo afectado en el puerto TCP 4786. Un ataque exitoso podría permitir al atacante causar un desbordamiento de búfer en el dispositivo afectado. Se ha asignado el identificador CVE-2018-0171 para esta vulnerabilidad de severidad crítica.

- **Validación de datos de entrada inadecuada**: Una vulnerabilidad en la funcionalidad Smart Install del Software Cisco IOS y Cisco IOS XE podría permitir a un atacante remoto sin autenticación desencadenar un reinicio en un dispositivo afectado, dando como resultado una condición de denegación de servicio (DoS). La vulnerabilidad se debe a una validación incorrecta de los datos del paquete. Un atacante podría explotar esta vulnerabilidad enviando un paquete a un dispositivo afectado en el puerto TCP 4786. Se ha asignado el identificador CVE-2018-0156 para esta vulnerabilidad de severidad crítica.

- **Validación de datos de entrada inadecuada**: Una vulnerabilidad en la opción 82 de la funcionalidad de encapsulación DHCP del software Cisco IOS y Cisco IOS XE podría permitir a un atacante remoto sin autenticación provocar un reinicio en el dispositivo afectado, causando una condición de denegación de servicio (DoS). Esta vulnerabilidad existe porque el software afectado implementa una validación incompleta de la entrada que recibe de paquetes DHCP Versión 4 (DHCPv4) desde los agentes de retransmisión. Un atacante podría explotar esta vulnerabilidad enviando un paquete DHCPv4 a un dispositivo afectado. Un ataque exitoso podría permitir al atacante causar un reinicio del dispositivo desencadenando una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2018-0174 para esta vulnerabilidad de severidad crítica.

- **Validación de datos de entrada inadecuada**: Una vulnerabilidad en la opción 82 de la funcionalidad de encapsulación DHCP del software Cisco IOS y Cisco IOS XE podría permitir a un atacante remoto sin autenticación provocar un reinicio en el dispositivo afectado, causando una condición de denegación de servicio (DoS). Esta vulnerabilidad existe porque el software afectado implementa una validación incompleta de la entrada que recibe de paquetes DHCP Versión 4 (DHCPv4) desde los agentes de retransmisión. Un atacante podría explotar esta vulnerabilidad enviando un paquete DHCPv4 a un dispositivo afectado. Un ataque exitoso podría permitir al atacante causar una un desbordamiento del heap, desencadenando una condición de denegación de servicio (DoS).Se ha asignado el identificador CVE-2018-0172 para esta vulnerabilidad de severidad crítica.

- **Validación de datos de entrada inadecuada**: Una vulnerabilidad en la funcionalidad del software de Cisco IOS y Cisco IOS XE que restablece la opción 82 de la encapsulación de paquetes DHCP Versión 4 (DHCPv4) podría permitir a un atacante remoto sin autenticación provocar un reinicio en el dispositivo afectado, dando lugar a una condición de denegación de servicio (DoS). Esta vulnerabilidad existe porque el software afectado implementa una validación incompleta de la entrada que recibe con información de la opción de encapsulación 82 de mensajes DHCPOFFER provenientes de servidores DCHPv4. Un atacante podría explotar esta vulnerabilidad enviando un paquete DCHPv4 al dispositivo afectado, que luego dicho dispositivo reenviará a un servidor DHCPv4. Cuando el software afectado procesa la información con la opción 82 que está encapsulada en la respuesta del servidor podría ocurrir un error. Un ataque exitoso podría permitir al atacante provocar un reinicio en el dispositivo afectado, desencadenando una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2018-0173 para esta vulnerabilidad de severidad crítica.

- **Validación de datos de entrada inadecuada**: Una vulnerabilidad en el módulo Internet Key Exchange Versión 2 (IKEv2) del software Cisco IOs y Cisco IOS XE podría permitir a un atacante remoto sin autenticar provocar una pérdida de memoria o un reinicio en el dispositivo afectado, desencadenado una condición de denegación de servicio (DoS). Esta vulnerabilidad se debe a un procesamiento incorrecto de ciertos paquetes IKEv2. Un atacante podría explotar esta vulnerabilidad enviado paquetes IKEv2 a un dispositivo afectado para ser procesados. Un ataque exitoso podría causar que un dispositivo afectado consuma memoria continuamente y en ocasiones reinicios, dando lugar a una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2018-0158 para esta vulnerabilidad de severidad crítica.

- **Incorrecta restricción de operaciones dentro de los límites de la memoria del buffer**: Una vulnerabilidad de desbordamiento de búfer en el subsistema LLDP del software Cisco IOS, Cisco IOS XE y Cisco IOS XR podría permitir a un atacante adyacente, sin autenticación provocar una condición de denegación de servicio (DoS) o la ejecución de código arbitrario con privilegios elevados. Se ha asignado el identificador CVE-2018-0167 para esta vulnerabilidad de severidad crítica.

- **Manejo incorrecto de parámetros de tipo cadena (string) procedentes de fuentes externas**: Una vulnerabilidad en la forma de manejar cadenas dentro del en el subsistema LLDP de Cisco IOS Software y Cisco IOS XR Software permitiría a un atacante conectado en una red adyacente, sin necesidad de estar autenticado causar una Denegación de Servicio o ejecutar código de forma arbitraria con privilegios elevados. Se ha asignado el código CVE-2018-0175 para esta vulnerabilidad de severidad alta.

- **Restricción de operaciones inadecuada en los límites de búfer de memoria**: Esta vulnerabilidad de tipo desbordamiento de búfer, en el subsistema LLDP de Cisco IOS Software y Cisco IOS XR Software permitiría a un atacante conectado en una red adyacente, sin necesidad de estar autenticado causar una Denegación de Servicio o ejecutar código de forma arbitraria con privilegios elevados. Se ha asignado el código CVE-2018-0167 para esta vulnerabilidad de severidad alta.

- **Vulnerabilidad en el manejo y gestión de errores (PK-ERRORS**): Existe una vulnerabilidad en la forma de gestionar los errores cuando una cabecera del protocolo BFD (Bidirectional Forwarding Detectio) está incompleta dentro del dicho paquete BFD. Un atacante remoto y sin necesidad de autenticación, podría enviar paquetes BFDF, especialmente malformados a través del Switch afectado, provocando una Denegación de Servicio debida a un reinicio forzoso del sistema. Se ha asignado el código CVE-2018-0155 para esta vulnerabilidad de severidad alta.

- **Incorrecta restricción de operaciones dentro de los límites de la memoria del buffer**: Una vulnerabilidad en el subsistema de calidad de servicio (QoS) de Cisco IOS y Cisco IOS XE podría permitir a un atacante remoto no autenticado causar una denegación de servicio (DoS) o ejecutar código arbitrario con máximos privilegios. La vulnerabilidad se debe a la comprobación incorrecta de ciertos valores en paquetes que están destinados al puerto 18999/udp del dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad para enviar paquetes maliciosos, cuando estos sean procesados, podría producirse una condición de desbordamiento de búfer. La explotación exitosa de esta vulnerabilidad podría permitir al atacante ejecutar código arbitrario en el dispositivo afectado con máximos privilegios. El atacante también podría aprovechar esta vulnerabilidad para hacer que el dispositivo realice una operación de ?reload?, causando una denegación de servicio temporal mientras el dispositivo se reinicia. Se ha asignado el código CVE-2018-0151 para esta vulnerabilidad de severidad crítica.

Identificadores reservados para las vulnerabilidades descritas en este aviso:

Rockwell Automation Stratix Industrial Managed Ethernet Switch: CVE-2018-0171, CVE-2018-0156, CVE-2018-0155, CVE-2018-0174, CVE-2018-0173, CVE-2018-0167, CVE-2018-0175

Rockwell Automation Stratix and ArmorStratix Switches: CVE-2018-0171, CVE-2018-0156, CVE-2018-0174, CVE-2018-0172, CVE-2018-0173, CVE-2018-0158, CVE-2018-0167, CVE-2018-0175

Rockwell Automation Stratix Services Router: CVE-2018-0158, CVE-2018-0151, CVE-2018-0167, CVE-2018-0175

Etiquetas: Actualización, Cisco, Sistema Operativo, Vulnerabilidad

---

Vulnerabilidad en la App de iOS SIMATIC WinCC OA Operator de Siemens

Fecha de publicación: 18/04/2018

Importancia: Media

Recursos afectados:

- SIMATIC WinCC OA Operator iOS App de Siemens, todas las versiones

Descripción:

Los investigadores Alexander Bolshev de IOActive e Ivan Yushkevich de Embedi se han coordinado con Siemens para gestionar esta vulnerabilidad. La App para iOS SIMATIC WinCC OA Operator estÃi afectada por una vulnerabilidad que permitiría a un atacante con acceso físico al dispositivo móvil, leer datos que no estÃin sujetos a un cifrado dentro del directorio de la aplicación.

Solución:

Siemens ha identificado las siguientes soluciones y mitigaciones específicas que sus clientes pueden aplicar para reducir el riesgo:

- Desactivar el botón que permite guardar la contraseña al iniciar y al cerrar la sesión después de cada espacio de trabajo.
- Seguir la guía de seguridad de SIMATIC WinCC OA para mantener la seguridad del entorno en SIMATIC WinCC OA. Esta guía puede descargarse en el siguiente enlace:

https://portal.etm.at/index.php?option=com_phocadownload&view=category&id=52:security&Itemid=81

Detalle:

- Exposición de datos sensibles: La App para iOS SIMATIC WinCC OA Operator de Siemens, no dispone de una protección suficiente sobre cierta información sensible (Datos de sesión para acceder al servidor, por ejemplo) de la aplicación. Un atacante con acceso físico al dispositivo móvil podría explotar esta vulnerabilidad para acceder a los datos con información sensible, que no estÃin sujetos a un cifrado dentro del directorio de la aplicación. Se ha reservado el identificador CVE-2018-4847 para esta vulnerabilidad.

Etiquetas: iOS, Móviles, Siemens, Vulnerabilidad

Desbordamiento de búfer en dispositivos CM600 y SAB600 de ABB

Fecha de publicación: 19/04/2018

Importancia: Alta

Recursos afectados:

- SAB600 3.5
- SAB600 3.5.1
- PCM600 2.4
- PCM600 2.4.0.1
- PCM600 2.4.0.2
- PCM600 2.4.1
- PCM600 2.4.1.1
- PCM600 2.4.1.2
- PCM600 2.4.1.3

Descripción:

Vladimir Dashchenko de Kaspersky Labs ha identificado varias vulnerabilidades de tipo desbordamiento de búfer que afectan a los productos CM600 y SAB600 de ABB. Un potencial atacante remoto no autenticado podría causar el cierre inesperado del sistema o la ejecución de código arbitrario.

Solución:

ABB informa que las vulnerabilidades se solucionan utilizando las siguientes versiones de producto:

- PCM600 2.5 o posterior
- SAB600 4.0 o posterior

Detalle:

El entorno de ejecución de Sentinel HASP incluido en los productos afectados dispone de varias vulnerabilidades de tipo desbordamiento de búfer que afectan tanto a la heap como a la stack. Un atacante podría explotar la vulnerabilidad cargando un fichero malicioso en Gemalto ACC (Admin Control Center) creando un desbordamiento de búfer. Estos desbordamientos podrían permitir a atacantes remotos la ejecución de código arbitrario o parar el proceso remoto provocando una denegación de servicio. Se han reservado los identificadores CVE-2017-11498, CVE-2017-11497, CVE-2017-11496 para estas vulnerabilidades.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Schneider Electric

Fecha de publicación: 24/04/2018

Importancia: Alta

Recursos afectados:

- Interfaz web de la estación de carga EVlink, todas las versiones anteriores a la v3.2.0-12_v1
- Wiser for KNX V2.1.0 y anteriores
- homeLYnk V2.0.1 y anteriores
- spaceLYnk V2.1.0 y anteriores

Descripción:

Joakim B. Hellum ha notificado a Schneider Electric una vulnerabilidad de severidad media de escalado de privilegio por la que un potencial atacante remoto podría ganar permisos administrativos. AdemÃis, el investigador independiente Jokin Guevara ha notificado otra vulnerabilidad de severidad alta de tipo *acceso FTP sin proteger* en el dispositivo Wiser for KNX (anteriormente homeLYnk / spaceLYnk) que podría permitir a un atacante sin autorización acceder al dispositivo.

Solución:

Schneider Electric ha publicado parches que solucionan las vulnerabilidades descritas en este aviso:

Escalada de privilegios:

https://www.schneider-electric.com/en/download/document/PHA6457000/

Acceso FTP sin proteger:

https://www.schneider-electric.com/en/download/document/FW2_1_1-HW_2_X_X-w4k/

Detalle:

- Mediante modificación de cookie en la estación de carga EVlink, un atacante remoto podría ganar privilegios de administrador sin la autenticación correcta para usuarios remotos. Se ha reservado el identificador CVE-2018-7778 para esta vulnerabilidad.
- Una configuración FTP débil o sin protección podría permitir el acceso a un atacante sin autorización. Se ha reservado el identificador CVE-2018-7779 para esta vulnerabilidad.

Etiquetas: Actualización, Navegador, Schneider Electric, Vulnerabilidad

---

Múltiples vulnerabilidades en WebAccess HMI Designer de Advantech

Fecha de publicación: 24/04/2018

Importancia: Media

Recursos afectados:

Advantech WebAccess HMI Designer

Descripción:

El investigador Steven Seeley de Source Incite ha identificado varias vulnerabilidades que podrían permitir a una atacante la ejecución remota de código en el producto afectado.

Solución:

Advantech no ha comunicado la forma de solucionar ninguna de las vulnerabilidades encontradas, sin embargo, el investigador que ha descubierto estas vulnerabilidades recomienda una estrategia de mitigación consistente en restringir la interacción con la aplicación a ficheros de confianza.

Detalle:

- Ejecución remota de código al analizar ficheros PM3 o durante la conversión de un archivo PM2 al formato PM3. Un atacante remoto podría ejecutar código arbitrario debido a alguna de las siguientes condiciones:
  - incorrecta validación de los datos de entrada
  - incorrecta validación de la longitud de los datos proporcionados por el usuario antes de copiarlos en un búfer de longitud fija
  - falta de comprobación en la existencia de un objeto antes de realizar operaciones en él

Etiquetas: 0day, Vulnerabilidad

Reutilización de Nonce en dispositivos de BD Pyxis

Fecha de publicación: 25/04/2018

Importancia: Media

Recursos afectados:

- BD Pyxis Anesthesia ES,

- BD Pyxis Anesthesia System 4000,
- BD Pyxis Anesthesia System 3500,
- BD Pyxis MedStation 4000 T2,
- BD Pyxis MedStation ES,
- BD Pyxis SupplyStation,
- BD Pyxis Supply Roller,
- BD Pyxis ParAssist System,
- BD Pyxis PARx,
- BD Pyxis CIISafe ? Workstation,
- BD Pyxis StockStation System, and
- BD Pyxis Parx handheld

Descripción:

El investigador Mathy Vanhoef de imec-DistriNet, KU Leuven, descubrió las vulnerabilidades KRACK y BD ha avisado de su posible afectación. Un potencial atacante podría manipular los datos de trÃifico, consiguiendo un descubrimiento parcial de comunicaciones cifradas o una inyección de trÃifico.

Solución:

BD ha implementado parches de terceros a través de su rutina de despliegue de parches que resuelve esta vulnerabilidad en la mayoría de dispositivos. Algunos dispositivos requieren de coordinación con BD. BD estÃi en contacto con los clientes para programar y desplegar los parches. AdemÃis, BD recomienda:

- Asegurarse de que las últimas actualizaciones se encuentran instaladas en los puntos de acceso Wifi
- Aplicar las medidas físicas apropiadas para prevenir los ataques que provienen del rango físico.
- Asegurarse que se disponen de copias de respaldo de los datos y de procesos de recuperación ante desastres.

Detalle:

Existe una vulnerabilidad en el protocolo WPA y WPA2 usado en toda la industria, afectado por ataques de reinstalación de claves conocidos como KRACK (Key Reinstallation Attacks).

El trÃifico de establecimiento en cuatro pasos usado en los protocolos Wi-Fi WPA y WPA2 se puede manipular para permitir la reutilización de nonce resultando en una reinstalación de la clave. Esto podría permitir a un potencial atacante dentro del alcance de la señal, ejecutar un ataque de hombre en el medio, reproducir, descifrar o falsificar tramas. Se han asignado los siguientes identificadores a esta vulnerabilidad: 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.

Etiquetas: Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en VGo Robot de Vecna

Fecha de publicación: 25/04/2018

Importancia: Alta

Recursos afectados:

- VGo Robot, todas las versiones anteriores a la 3.0.3.52164

Descripción:

El investigador Dan Regalado de Zingbox ha identificado varias vulnerabilidades de tipo inyección de comandos y transmisión de datos en claro que afectan a los productos VGo Robot de Vecna. Un potencial atacante remoto podría capturar las actualizaciones de firmware realizadas en red y conseguir ejecución remota de código.

Solución:

Vecna ha publicado una actualización recomendada para mitigar estas vulnerabilidades. Recomienda el siguiente proceso de actualización:

- De forma predeterminada, VGo tiene activadas las actualizaciones automÃiticas, por lo que todas las actualizaciones se realizan automÃiticamente cuando estÃi disponible el acceso a Internet. Si el VGo estÃi apagado o en uso, aparecerÃi un mensaje en la pantalla que le preguntarÃi si puede actualizarse en el próximo uso.
- Si una unidad VGo tiene actualizaciones automÃiticas desactivadas, la actualización no se descargarÃi (sin embargo, se mostrarÃi un aviso sobre la actualización en la pantalla del VGo). Vecna recomienda que las actualizaciones automÃiticas estén activadas.

Detalle:

- Inyección de comandos: Un potencial atacante en redes adyacentes podría realizar una inyección de comandos. Se ha reservado el identificador CVE-2018-8866 para esta vulnerabilidad.
- Transmisión en claro: Un potencial atacante podría capturar las actualizaciones de firmware desde una red adyacente. Se ha reservado el identificador CVE-2018-8860 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Desbordamiento de búfer en módem 2G de Intel

Fecha de publicación: 25/04/2018

Importancia: Alta

Recursos afectados:

- Intel XMM71xx
- Intel XMM72xx
- Intel XMM73xx

- Intel XMM74xx
- Sofia 3G
- Sofia 3G-R
- Sofia 3G-R W

Descripción:

El Dr. Ralph Phillip Weinmann y el Dr. Nico Golde de la empresa Comsecuris, han reportado esta vulnerabilidad de tipo desbordamiento de búfer a la empresa Intel que, a su vez, ha reportado la vulnerabilidad al NCCIC. La explotación por parte de un atacante remoto de esta vulnerabilidad permitiría a este la ejecución remota de código en el dispositivo afectado.

Solución:

Intel ha publicado una nueva versión de firmware para corregir la vulnerabilidad en los dispositivos afectados. Los usuarios que posean dispositivos afectados, deben consultar con sus proveedores la incorporación de esta actualización y aplicarla lo antes posible.

Detalle:

Un atacante remoto podría aprovechar esta vulnerabilidad de tipo desbordamiento de búfer existente en el módulo de procesamiento ETWS (Earthquake and Tsunami Warning System) para ejecutar código arbitrario a través de una red adyacente. Se ha reservado el identificador CVE-2018-3624 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Microsoft, Vulnerabilidad

Múltiples vulnerabilidades en cámaras Pelco Sarix Pro de Schneider Electric

Fecha de publicación: 26/04/2018

Importancia: Alta

Recursos afectados:

- Primera generación de Pelco Sarix Pro con firmware versión anterior a la 3.29.69

Descripción:

El investigador Giri Veeraraghavan Veda de Gulf Business Machines y el grupo Weapon x, han informado a Schneider Electric de 3 vulnerabilidades de severidad alta de los siguientes tipos: desbordamiento de búfer, escalada de privilegios y divulgación de información que afectan a sus cÃ¡maras Pelco Sarix Pro. Un potencial atacante autenticado podría llegar a obtener contraseñas de usuarios, provocar una denegación de servicio o realizar un desbordamiento de búfer.

Solución:

Schneider Electric ha publicado la versión 3.29.69 del firmware que soluciona estas vulnerabilides que puede descargarse desde:

https://www.pelco.com/search#keyword/v3.29.69/tab/documents

Detalle:

Las vulnerabilides identificadas son las siguientes:

- Desbordamiento de búfer: Existe un desbordamiento de búfer en el programa ?set? del cgi. Se ha reservado el identificador CVE-2018-7780 para esta vulnerabilidad.
- Divulgación de contraseñas y escalada de privilegios: Un potencial atacante autenticado podría enviar peticiones especialmente manipuladas y podría ver las contraseñas en claro, desembocando en una escalada de privilegios. Se ha reservado el identificador CVE-2018-7781 para esta vulnerabilidad.
- Divulgación de contraseñas: Un potencial atacante autenticado podría ver las contraseñas en claro. Se ha reservado el identificador CVE-2018-7782 para esta vulnerabilidad.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Desbordamiento de búfer en PMSoft de Delta Electronics

Fecha de publicación: 27/04/2018

Importancia: Alta

Recursos afectados:

- PMSoft v 2.10 y anteriores

Descripción:

El investigador Ghirmay Desta, trabajando con Zero Day Initiative de Trend Micro, ha informado de varios desbordamientos de búfer que afectan al software PMSoft de Delta Electronics. Un potencial atacante local podría aprovecharse de estas vulnerabilidades para ejecutar código arbitrario o hacer que la aplicación falle.

Solución:

Delta Electronics recomienda a los usuarios afectados actualizar a PMSoft v2.1, que estÃ¡ disponible desde el 22 de marzo de 2018. La descarga puede encontrarse en el siguiente enlace:

www.deltaww.com/Products/PluginWebUserControl/downloadCenterCounter.aspx?DID=2092&DocPath=1&hl=en-US

Detalle:

La aplicación tiene múltiples vulnerabilidades de tipo desbordamiento de búfer donde un fichero .ppm puede introducir un valor mÃis largo que el que permite leer el búfer de tamaño fijo definido en PMSoft. Esto provoca que el búfer se sobrescriba, lo que puede permitir la ejecución de código arbitrario o hacer que la aplicación falle. Se ha reservado el identificador CVE-2018-8839 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Desbordamiento de Búfer en LeviStudio HMI Editor y PI Studio HMI Project Programmer de WECON Technology Co

Fecha de publicación: 27/04/2018

Importancia: Media

Recursos afectados:

- WECON LeviStudioU Version 1.10, componente de las versiones de WECON LeviStudioU 1.8.29 y anteriores
- PI Studio HMI Project Programmer Build: 11 de noviembre 2017 y anteriores

Descripción:

Los investigadores Sergey Zelenyuk de RVRT y Michael DePlante de Leahy Center of Digital Investigation at Champlain College, en colaboración con Zero Day Initiative de Trend Micro, han identificado una vulnerabilidad de desbordamiento de búfer que afectan a LeviStudio HMI Editor y PI Studio HMI Project Programmer de WECON Technology Co. Esto podría permitir la ejecución remota de código.

Solución:

WECON recomienda descargarse la última versión disponible. La descarga puede encontrarse en el siguiente enlace:

http://wecon-disk.oss-ap-southeast-1.aliyuncs.com/LeviStudioU20180420 TEST.exe

Detalle:

- Desbordamiento de búfer basado en pila: un fichero especialmente manipulado puede provocar una sobreescritura de la pila al ser abierto por estas aplicaciones, permitiendo la ejecución remota de código. Se ha reservado el identificador CVE-2018-7527 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad