Boletín de Agosto de 2018

Avisos de Sistemas de Control Industrial

Hash de contraseñas débil en DVW-3200N de Davolink

Fecha de publicación: 01/08/2018

Importancia: Crítica

Recursos afectados:

- DVW-3200N, todas las versiones anteriores a 1.00.06

Descripción:

Ankit Anubhav de NewSky Security ha descubierto una vulnerabilidad de tipo de almacenamiento de hash de contraseñas elaborados sin el suficiente esfuerzo computacional. Un potencial atacante remoto podría obtener las contraseñas del dispositivo.

Solución:

Davolink ha liberado una nueva versión de firmware que corrige esta vulnerabilidad. Puede descargarse en http://www.davolink.co.kr/sys/bbs/board.php?bo_table=0403&wr_id=50.

Detalle:

Los dispositivos afectados generan hash de contraseñas débiles que son fácilmente rompibles, permitiendo a un potencial atacante obtener las contraseñas del dispositivo. Se ha reservado el identificador CVE-2018-10618 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en productos AVEVA

Fecha de publicación: 01/08/2018

Importancia: Crítica

Recursos afectados:

- Wonderware License Server versión v4.0.13100 y anteriores (hace uso de Flexara Imgrd versión 11.13.1.1 y anteriores). Solo los usuarios con la característica Counted Licenses con ?ArchestrAServer.lic? están afectados.
- InTouch Access Anywhere 2017 Update 2 y anteriores. Las versiones vulnerables de jQuery son aquellas anteriores a la versión 3.0.0.

Descripción:

Security Team de Google y un investigador anónimo han identificado varias vulnerabilidades de tipo neutralización inapropiada de los datos de entrada y restricción inadecuada en los límites del búfer de memoria en productos de AVEVA. Un potencial atacante podría obtener información sensible, ejecutar código Javascript y HTML o código remoto con privilegios de administrador.

Solución:

AVEVA recomienda a los usuario afectados instalar los parches ?InTouch Access Anywhere 2017 Update 2b? y "Hotfix Wonderware License Server VU-485744? o posteriores, según el producto afectado.

Detalle:

- Restricción inadecuada en los límites del búfer de memoria: un desbordamiento de búfer en lmgrd y el demonio del vendedor de Flexera FlexNet Publisher podría permitir a un atacante remoto la ejecución de código arbitrario mediante un paquete manipulado,

permitiendo la ejecución de código remoto con privilegios de administrador. Se ha asignado el identificador CVE-2015-8277 para esta vulnerabilidad.
- Neutralización inadecuada de los datos de entrada durante la generación de la página web (cross-site-scripting): la librería jQuery es vulnerable a ataques cross-site scripting (XSS) cuando una petición Ajax de dominio cruzado es realizada sin la opción dataType, lo que provoca que se ejecuten respuestas de texto/javascript. Se ha asignado el identificador CVE-2015-9251 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Divulgación de información en Metasys y BCPro de Johnson Controls

Fecha de publicación: 01/08/2018

Importancia: Media

Recursos afectados:

- Metasys System, Versión 8.0 y anteriores
- BCPro (BCM), todas las versiones anteriores a la 3.0.2

Descripción:

El investigador Dan Regalado de Zingbox ha identificado una vulnerabilidad de tipo divulgación de información que afecta a productos de Johnson Controls. Un potencial atacante podría obtener información técnica.

Solución:

La vulnerabilidad en Metasys se corrigió en la versión v8.1, no obstante, se debe actualizar a la última versión del producto, versión 9.0. Los usuarios de BCPro Workstation deben actualizar a la versión v3.0 para remediar la vulnerabilidad y los de BACnet Router y Gateway deben actualizar a la versión 3.0.2.

Detalle:

Esta vulnerabilidad es producto de la inadecuada gestión de errores de las comunicaciones con el servidor basadas en HTTP, las cuales pueden permitir a un atacante obtener información técnica. Se ha asignado el identificador CVE-2018-10624 a esta vulnerabilidad.

Etiquetas: Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en CNCSoft y ScreenEditor de Delta Electronics

Fecha de publicación: 08/08/2018

Importancia: Alta

Recursos afectados:

- CNCSoft Versión 1.00.83 y anteriores
- ScreenEditor Versión 1.00.54

Descripción:

Mat Powell trabajando en colaboración con Zero Day Initiative de Trend Micro, han reportado estas vulnerabilidades al NCCIC/ICS-CERT, cuya explotación exitosa permitiría a un atacante la ejecución de código remoto con privilegios de administrador.

Solución:

Delta Electronics recomienda actualizar a la última versión de CNCSoft, la v1.01.09 y restringir la interacción con la aplicación a ficheros de confianza.

Detalle:

- Múltiples vulnerabilidades de desbordamiento de búfer basado en la pila hacen que el software falle debido a la falta de validación de entrada del usuario antes de copiar los datos de los archivos del proyecto a la pila. Se ha asignado el identificador CVE-2018-10636 para esta vulnerabilidad.
- Dos vulnerabilidades de lectura fuera de límites provocan el cierre inesperado debido a la falta de validación de entrada del usuario para procesar los archivos del proyecto. Se ha asignado el identificador CVE-2018-10598 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en productos Medtronic

Fecha de publicación: 08/08/2018

Importancia: Media

Recursos afectados:

- MMT - 508 MiniMed insulin pump

- MMT - 522 / MMT - 722 Paradigm REAL-TIME
- MMT - 523 / MMT - 723 Paradigm Revel
- MMT - 523K / MMT - 723K Paradigm Revel
- MMT - 551 / MMT - 751 MiniMed 530G
- 24950 MyCareLink Monitor, todas las versiones.
- 24952 MyCareLink Monitor, todas las versiones.

Descripción:

Billy Rios, Jesse Young y Jonathan Butts de Whitescope LLC han reportado estas vulnerabilidades al NCCIC/ICS-CERT que podrían permitir a un atacante remoto reinyectar comunicaciones inalámbricas capturadas y provocar la distribución de insulina (bolus) en un paciente. Por otro lado, si un atacante obtuviera acceso físico a los dispositivos MyCareLink sería capaz de obtener las credenciales de cada producto. Posteriormente, se podría aprovechar esta vulnerabilidad para cargar datos incorrectos a la red de Medtronic CareLink.

Solución:

- En cuanto a las vulnerabilidades que afectan a los dispositivos MMT, Medtronic no va a desarrollar una actualización para estas vulnerabilidades debido a que, si un usuario nunca ha programado o usado un control remoto, no es susceptible a ser atacado. Además, si el usuario desactiva la opción remota o desactiva la opción ?easy bolus? en su bomba de insulina, no sería susceptible al ataque.
- Para las vulnerabilidades que afectan a los dispositivos MyCareLink Monitor, Medtronic ha realizado actualizaciones en el servidor para abordar la vulnerabilidad identificada en este aviso de verificación insuficiente. Además, está implementando mitigaciones adicionales en el lado del servidor para mejorar la integridad y autenticidad de los datos. Por otro lado, Medtronic recomienda a los usuarios tomar medidas defensivas adicionales para minimizar el riesgo de explotación. Específicamente, los usuarios deberían:
  - Mantener un buen control físico sobre el monitor del hogar.
  - Utilizar únicamente monitores domésticos obtenidos directamente de su proveedor de atención médica o de un representante de Medtronic para garantizar la integridad del sistema.

  Por último, puede encontrarse más información publicada por Medtronic en el siguiente enlace:
  https://www.medtronic.com/security

Detalle:

- Las comunicaciones entre la bomba y los accesorios inalámbricos en los modelos MNT son transmitidas mediante texto en claro. Un atacante con la habilidad suficiente podría capturar estas transmisiones y extraer información sensible como los números serie del dispositivo. Se ha asignado el identificador CVE-2018-10634 para esta vulnerabilidad.
- Los dispositivos MMT anteriormente identificados, cuando son emparejados con un controlador remoto y tienen las opciones ?easy bolus? y ?remote bolus? activadas (no son opciones por defecto), son vulnerables a un ataque de captura-repetición. Un atacante podría capturar las comunicaciones inalámbricas entre el controlador remoto y la bomba y repetirlas para provocar una distribución de un bolo de insulina. Se ha asignado el identificador CVE-2018-12781 para esta vulnerabilidad.
- El servicio de actualización de los productos MyCareLink Monitor afectados, no verifica suficientemente la autenticidad de los datos cargados. Un atacante que obtuviera las credenciales por producto del monitor y la información del dispositivo cardíaco implantable podría cargar datos no válidos a la red de Medtronic CareLink. Se ha asignado el identificador CVE-2018-10626 para esta vulnerabilidad.
- Los productos MyCareLink Monitor afectados utilizan credenciales por producto que son almacenadas en un formato recuperable. Un atacante podría usar estas credenciales para autenticación en la red y encriptación de datos locales en reposo. Se ha asignado el identificador CVE-2018-10622 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en productos de Siemens

Fecha de publicación: 08/08/2018

Importancia: Alta

Recursos afectados:

- Automation License Manager 5, todas las versiones anteriores a la 5.3.4.4.
- Automation License Manager 6, todas las versiones anteriores a la 6.0.1 (sólo afectado por la vulnerabilidad CVE-2018-11455).
- SIMATIC STEP 7 (TIA Portal) y WinCC (TIA Portal) V10, V11, V12, todas las versiones.
- SIMATIC STEP 7 (TIA Portal) y WinCC (TIA Portal) V13, todas las versiones.
- SIMATIC STEP 7 (TIA Portal) y WinCC (TIA Portal) V14, todas las versiones anteriores a la V14 SP1 Update 6.
- SIMATIC STEP 7 (TIA Portal) y WinCC (TIA Portal) V15, todas las versiones anteriores a la V15 Update 2.
- MindConnect IoT2040, todas las versiones anteriores a la V03.01.
- MindConnect Nano (IPC227D), todas las versiones anteriores a la V03.01.
- SIMATIC ET 200SP Open Controller CPU 1515SP PC (OC1), todas las versiones anteriores a la V2.1.
- SIMATIC HMI WinCC Flexible, todas las versiones.
- SIMATIC IPC DiagBase, todas las versiones.
- SIMATIC IPC DiagMonitor, todas las versiones.
- SIMATIC S7-1200, todas las versiones.
- SIMATIC S7-1500, todas las versiones anteriores a la V2.5.2.
- SIMATIC S7-1500 Software Controller, todas las versiones.
- SIMATIC WinCC OA V3.14, todas las versiones.
- SIMATIC WinCC OA V3.15, todas las versiones.
- SIMATIC WinCC OA V3.16, todas las versiones.
- SINUMERIK Integrate Access MyMachine service engineer client, como parte de la suite Sinumerik Integrate Product, afectada la versión V4.1.7 y anteriores.
- SINUMERIK Integrate Operate Client, como parte de la suite Sinumerik Integrate Product, versiones 2.0.11/3.0.11 y todas las anteriores a ellas.

Descripción:

Los investigadores Vladimir Dashchenko de Kaspersky Lab, Younes Dragoni de Nozomi Networks, el equipo del ICS-CERT y Siemens, han participado en el descubrimiento y gestión de varias vulnerabilidades de tipo salto de directorio, gestión inapropiada de permisos, envío de paquetes especialmente diseñados y problemas relacionados con OpenSSL. La vulnerabilidad relacionada con el OpenSSL permitiría a un atacante remoto obtener la información intercambiada bajo un canal ?seguro? con OpenSSL comprometiendo la confidencialidad. Por otro lado, un atacante podría llegar a ejecutar código remoto o modificar la estructura de carpetas en los dispositivos afectados mediante la explotación de las dos vulnerabilidades remanentes.

Solución:

En el caso de los siguientes productos, hay disponible un nueva versión de software que mitiga las vulnerabilidades:

- Automation License Manager 5, actualizar a V5.3.4.4.
- Automation License Manager 6, actualizar a V6.0.1.

En el caso de no poder actualizar el producto afectado, el fabricante recomienda restringir el acceso a la red desde la que se puede acceder al sistema que contenga este software.

- SIMATIC STEP 7 (TIA Portal) y WinCC (TIA Portal) V14, actualizar a la V14 SP1 Update 6.
- SIMATIC STEP 7 (TIA Portal) y WinCC (TIA Portal) V15, actualizar a la V15 Update 2 o versiones posteriores.
- Para las versiones 10, 11, 12 y 13 de SIMATIC STEP 7 (TIA Portal) y WinCC (TIA Portal) afectadas el fabricante recomienda aplicar las siguientes mitigaciones:
  - Restringir el acceso al sistema operativo sólo a personas autorizadas.
  - Validar los ficheros GSD para verificar su legitimidad y procesar los ficheros GSD sólo de fuentes confiables.
- MindConnect IoT2040, actualizar a la V03.01 o posteriores con el Mindsphere web frontend.
- MindConnect Nano (IPC227D), actualizar a la V03.01 o posteriores con el Mindsphere web frontend.
- SIMATIC S7-1500, actualizar a la V2.5.2.
- SINUMERIK Integrate Access MyMachine service engineer client, actualizar a la V4.1.8, instalando la última versión de la suite Sinumerik Integrate Product.
- SINUMERIK Integrate Operate Client, actualizar a la V2.0.12/3.0.12, instalando la última versión de la suite Sinumerik Integrate Product.
- S7-1200. El fabricante recomienda deshabilitar el servidor web si este no se está utilizando o limitar el acceso al mismo vía Ethernet/PROFINET puerto/interfaz si es posible. Las configuraciones pueden hacerse en ?General/Web server access?.
- Para todos los productos a los que no se ha hecho referencia aún en las mitigaciones, el fabricante recomienda restringir el acceso a los productos afectados utilizando mecanismos apropiados como por ejemplo la configuración de un cortafuegos.

Detalle:

- **Salto de directorio** (Automation License Manager). La explotación exitosa de esta vulnerabilidad, permitiría a un atacante mover archivos de forma arbitraria, pudiendo llegar a realizar una ejecución remota de código comprometiendo la confidencialidad, integridad y disponibilidad del sistema. La explotación de esta vulnerabilidad requiere que el atacante se encuentre en la misma red que el producto afectado sin necesidad de privilegios o condiciones especiales del sistema, pero, siendo necesaria la interacción de un usuario víctima. Se ha asignado el identificador CVE-2018-11455 para esta vulnerabilidad.
- **Envío de paquetes especialmente diseñados** (Automation License Manager). Un atacante con acceso a la red donde se encuentra el producto afectado podría enviar paquetes especialmente diseñados para determinar si es posible acceder o no a un puerto de red en otro sistema remoto. Este hecho permite a un atacante realizar un escaneo de red básico usando una máquina víctima para obtener información. Para explotar esta vulnerabilidad, el atacante ha de estar conectado a la misma red que el producto afectado, no necesita privilegios y no requiere de interacción de usuarios. Se ha asignado el identificador CVE-2018-11456 para esta vulnerabilidad.
- **Gestión de permisos inapropiada**. Los permisos que poseen algunos archivos en la instalación por defecto del TIA Portal pueden permitir a un posible atacante con acceso local al sistema insertar archivos especialmente diseñados que pueden evitar el inicio del TIA Portal originando así una denegación de servicio o la ejecución local de código malicioso. Para la explotación exitosa de esta vulnerabilidad no se requieren permisos especiales, pero sí que la víctima intente iniciar el TIA Portal tras la manipulación de los archivos. Se ha asignado el identificador CVE-2018-11453 para esta vulnerabilidad.
- **Gestión de permisos inapropiada**. Los permisos que poseen algunos archivos en la instalación por defecto del TIA Portal pueden permitir a un posible atacante con acceso local al sistema manipular recursos que pueden ser transferidos a otros dispositivos y posteriormente ser ejecutados. Para la explotación exitosa de esta vulnerabilidad no se requieren permisos especiales, pero sí que la víctima transfiera los archivos manipulados a otro dispositivo (PG). Se ha asignado el identificador CVE-2018-11454 para esta vulnerabilidad.
- **OpenSSL**. En OpenSSL v1.0.2 se introdujo un mecanismo de ?error state?. Este mecanismo no funciona de forma correcta cuando se llama a las funciones SSL_red() o SSL_write(). Este hecho podría resultar en un envío de datos sin cifrado en la capa SSL/TLS. La explotación exitosa de esta vulnerabilidad requiere que un atacante cause un error durante el establecimiento de la conexión (handshake) bajo SSL/TLS y que la aplicación haga las llamadas a SSL_read() o SSL_write() después de recibir el error. No se requieren de privilegios o interacción del usuario para explotar esta vulnerabilidad. Se ha asignado el identificador CVE-2017-3737 para esta vulnerabilidad.

Etiquetas: Navegador, Privacidad, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en Zipabox de Zipato

Fecha de publicación: 09/08/2018

Importancia: Alta

Recursos afectados:

- Zipato Zipabox (smart home controller)

Descripción:

Andrey Muravitsky, del Critical Infrastructure Defense Team de Kaspersky Lab ICS CERT ha reportado varias vulnerabilidades a Zipato. Un atacante remoto podría obtener información sensible que expandiera la superficie de ataque, explotara una vulnerabilidad o extrajera sin autenticación, contraseñas en texto en claro pudiendo llegar a tomar el control de todo el hogar inteligente gestionado por los dispositivos afectados.

Solución:

Por el momento no se encuentra ninguna solución disponible.

Detalle:

- **Divulgación de información sensible**: un atacante sin autenticación podría ser capaz de extraer información sensible sobre los dispositivos Zipabox disponibles y su información técnica. Se ha asignado el identificador CVE-2018-15125 para esta vulnerabilidad.
- **Algoritmo de hash débil**: un atacante sin autenticación podría aprovechar esta vulnerabilidad para extraer contraseñas de texto en claro. Se ha asignado el identificador CVE-2018-15124 a esta vulnerabilidad.
- **Almacenamiento de configuración inseguro**: un atacante sin autenticación podría aprovechar esta vulnerabilidad para tomar el control de todo el hogar inteligente. Se ha asignado el identificador CVE-2018-15123 para esta vulnerabilidad.

Etiquetas: Privacidad, Vulnerabilidad

Múltiples vulnerabilidades en router 4G LTE Light Industrial M2M de NetComm Wireless

Fecha de publicación: 10/08/2018

Importancia: Crítica

Recursos afectados:

- Router 4G LTE Light Industrial M2M (NWL-25) con versión de firmware 2.0.29.11 y anteriores.

Descripción:

El investigador Aditya K. Sood ha reportado al ICS-CERT varias vulnerabilidades de tipo Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF) y exposición de información sensible que afectan al router 4G LTE Light Industrial M2M del fabricante NetComm Wireless. La explotación exitosa de estas vulnerabilidades permitiría a un atacante remoto obtener información sensible del dispositivo afectado.

Solución:

NetComm Wireless ha publicado una nueva versión de firmware (NWL-25 versión de firmware 2.0.29.12_C) para solventar las vulnerabilidades que afectan al router 4G LTE Light Industrial M2M.

Enlace de descarga: https://support.netcommwireless.com/product/nwl-25#Firmware

Detalle:

- El dispositivo permite acceder a los ficheros y perfiles de configuración sin necesidad de que un usuario este registrado. Se ha asignado el identificador CVE-2018-14782 para esta vulnerabilidad.
- El dispositivo no dispone de medidas de seguridad en el tratamiento de las sesiones. Esto permitiría a un atacante enviar una petición especialmente formada para que una víctima registrada dentro del producto afectado cambie la contraseña del dispositivo de forma remota. Se ha asignado el identificador CVE-2018-14783 para esta vulnerabilidad.
- Vulnerabilidad de cross-site scripting podría permitir a un atacante remoto ejecutar código arbitrario en el dispositivo. Se ha asignado el identificador CVE-2018-14784 para esta vulnerabilidad.
- El directorio de ficheros que posee el dispositivo se encuentra accesible sin necesidad de autenticación. Un atacante podría aprovecharse de esta vulnerabilidad para obtener información del dispositivo afectado y elaborar ataques más complejos. Se ha asignado el identificador CVE-2018-14785 para esta vulnerabilidad.

Etiquetas: Gestor de contenidos, Navegador, Privacidad, Vulnerabilidad

Múltiples vulnerabilidades en TSW-X60 y MC3 de Crestron

Fecha de publicación: 10/08/2018

Importancia: Crítica

Recursos afectados:

- TSW-X60 todas las versiones anteriores a 2.001.0037.001
- MC3 todas las versiones anteriores a 1.502.0047.001

Descripción:

Jackson Thuraisamy en colaboración con Security Compass, ha reportado algunas de estas vulnerabilidades a Crestron. Por otra parte, Ricky ?HeadlessZeke? Lawshae, en colaboración con Zero Day Initiative de Trend Micro, ha reportado más vulnerabilidades al NCCIC/ICS-CERT. Una explotación exitosa de estas vulnerabilidades permitiría la ejecución remota de código con escalada de privilegios en el sistema.

Solución:

Crestron recomienda a los usuarios actualizar sus dispositivos a la última versión de firmware disponible en:

- TSW-X60 (inicio de sesión necesario): https://www.crestron.com/en-US/Software-Firmware/Firmware/Touchpanels/TSW-560-TSW-760-TSW-1060/2-001-0040-01
- MC3 (inicio de sesión necesario): https://www.crestron.com/en-US/Software-Firmware/Firmware/Touchpanels/TSW-560-TSW-760-TSW-1060/2-001-0040-01

Por último, Crestron también recomienda a los usuarios que consulten la ayuda en línea de Crestron para obtener información sobre esta y otras vulnerabilidades (Artículo #5471). La información para el bastionado de dispositivos se encuentra disponible en el Artículo #5571.

Detalle:

- Vulnerabilidad de inyección de comandos en S.O podría permitir la ejecución remota de código sin autenticación mediante un servicio Bash Shell en Crestron Toolbox Protocol (CTP). Esta vulnerabilidad afecta únicamente a los dispositivos TSW-X60. Se ha asignado el identificador CVE-2018-11228 para esta vulnerabilidad.
- Vulnerabilidad de Inyección de comandos en S.O. podría permitir la ejecución remota de código sin autenticación mediante la inyección de comandos en Crestron Toolbox Protocol (CTP). Esta vulnerabilidad afecta únicamente a los dispositivos TSW-X60. Se ha asignado el identificador CVE-2018-11229 para esta vulnerabilidad.
- Los dispositivos se envían con la autenticación deshabilitada por parte del fabricante y no hay ninguna indicación para que los usuarios puedan aplicar medidas de seguridad y habilitar esta opción. Cuando el dispositivo afectado es comprometido, el acceso a la consola CTP queda abierto. Se ha asignado el identificador CVE-2018-10630 para esta vulnerabilidad.
- Las contraseñas para cuentas de administración se pueden averiguar usando información accesible por usuarios con privilegios normales. Los atacantes podrían descifrar estas contraseñas, para después ejecutar llamadas a API ocultas y escapar de la sandbox que posee la consola CTP con privilegios elevados. Se ha asignado el identificador CVE-2018-13341 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en Intel Management Engine de productos Moxa

Fecha de publicación: 10/08/2018

Importancia: Crítica

Recursos afectados:

- DA-820 Series versiones anteriores a V1.10S03
- MC-7200-DC-CP Series versiones anteriores a V1.20S01
- MC-7200-MP Series versiones anteriores a V1.30S01
- EXPC-1519 Series versiones anteriores a V1.20S02
- DA-720 Series versiones anteriores a V1.30S00

Descripción:

Moxa ha identificado los productos de su portfolio que se encuentran afectados por las vulnerabilidades de Intel Management Engine (CVE-2017-5689, CVE-2017-5705, CVE-2017-5708, CVE-2017-5711, CVE-2017-5712) y ha publicado una actualización de BIOS para cada producto afectado que corrige estas vulnerabilidades.

Solución:

Moxa ha identificado cuales de sus productos se encuentran afectados y ha emitido una actualización de firmware. Cualquier producto que no esté en la lista no se verá afectado por las vulnerabilidades mencionadas en este documento. Moxa recomienda que las personas que hayan comprado los productos afectados reciban asistencia a través del Servicio al cliente global de Moxa y actualicen a la última versión de BIOS:

- DA-820 Series versiones anteriores a V1.10S03
- MC-7200-DC-CP Series versiones anteriores a V1.20S01
- MC-7200-MP Series versiones anteriores a V1.30S01
- EXPC-1519 Series versiones anteriores a V1.20S02
- DA-720 Series versiones anteriores a V1.30S00

Detalle:

En mayo de 2017, varios investigadores anunciaron una vulnerabilidad según la cual, un atacante que no debiera tener acceso a una red podría obtener privilegios del sistema para suministrar SKUs de administración de Intel y un atacante local podría proporcionar funciones de administración para obtener privilegios de red o del sistema local en SKU de administración de Intel (CVE-2017-5689). En la segunda mitad de 2017, investigadores identificaron múltiples vulnerabilidades relacionadas con Intel Management Engine. (CVE-2017-5705, CVE-2017-5708, CVE-2017-5711, CVE-2017-5712).

Etiquetas: Vulnerabilidad

Evasión de autenticación en eSOMS de ABB

Fecha de publicación: 13/08/2018

Importancia: Crítica

Recursos afectados:

- eSOMS, versión 6.0.2

Descripción:

Un investigador anónimo ha reportado una vulnerabilidad de tipo evasión de autenticación que afecta a los productos eSOMS de ABB que pordría permitir el acceso a la aplicación como usuario legítimo.

Solución:

ABB se encuentra trabajando en el parche 6.0.3 que solucionará esta vulnerabilidad añadiendo una comprobación que evite la autenticación en eSOMS sin contraseña independientemente de la configuración del servidor LDAP.

Mientras tanto, se aconseja a los clientes asegurarse que la opción ?Unauthenticated Authentication? se encuentra deshabilitada en las opciones de configuración LDAP. En el archivo web.config de eSOMS hay que asegurarse de que solo los siguientes valores clave están configurados: ?LDAP_Path?, ?LDAP_User_Search? y ?LDAP_SSL_Enabled?.

Detalle:

Los servidores de autenticación LDAP se pueden configurar para permitir autenticación anónima. Cuando se configura autenticación LDAP en eSOMS, un usuario puede iniciar sesión sin contraseña si las siguientes opciones están configuradas:

- El servidor LDAP está configurado para permitir ?Unauthenticated Authentication?
- Cuando se configuran más valores clave aparte de ?LDAP_Path?, LDAP_User_Search? y ?LDAP_SSL_Enabled? en el fichero web.config

Etiquetas: Vulnerabilidad

Denegación de servicio en ILC 1x1 ETH de Phoenix

Contact

Fecha de publicación: 14/08/2018

Importancia: Alta

Recursos afectados:

- Phoenix Contact ILC 131, 151, 171, 191 ETH, todas sus versiones de firmware.

Descripción:

Matthias Niedermaier y Florian Fischer de Hochschule Augsburg y Jan-Ole Malchow de Freie Universita?t Berlin han reportado una vulnerabilidad de tipo denegación de servicio. Un potencial atacante podría saturar la red en la que se encuentra el dispositivo haciendo que éste no llegue a iniciarse.

Solución:

Se recomienda a los clientes que utilicen Phoenix Contact ILC 1x1 que operen los dispositivos en redes cerradas o protegidos por un cortafuegos adecuado.

Para obtener información detallada sobre medidas para proteger los dispositivos de red, Phoenix Contact recomienda visitar el siguiente enlace:

https://www.phoenixcontact.com/assets/downloads_ed/local_pc/web_dwl_technical_info/ah_en_industrial_security_107913_en_01.pdf

Detalle:

El procesamiento del programa IEC 61131 puede ser muy lento o llegar a detenerse si la cantidad de tráfico en la red es muy elevada.

El procesamiento de la carga en red requiere tanta potencia de CPU que la operación de todas las funciones del dispositivo, incluido el programa 61131, se ralentizará. Esto puede afectar a la tarea de automatización. Una vez que se elimina la saturación de la red, el dispositivo ILC vuelve a su estado normal.

Etiquetas: Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en IntelliSpace Cardiovascular de Philips

Fecha de publicación: 16/08/2018

Importancia: Alta

Recursos afectados:

- IntelliSpace Cardiovascular (ISCV), versiones 3.1 y anteriores.
- Xcelera versiones 4.1 y anteriores.

Descripción:

Philips ha reportado varias vulnerabilidades en sus productos de gestión de información IntelliSpace Cardiovascular (ISCV). Un potencial atacante con acceso local y autenticado en la aplicación, podría aprovecharse de estas vulnerabilidades para escalar privilegios dentro del servidor ISCV/Xcelera o ejecutar código arbitrario.

Solución:

- Una de las vulnerabilidades publicadas que aplica a las versiones ISCV versión 2.X y anteriores, es corregida en la versión 3.1, los usuarios pueden ponerse en contacto con el equipo de soporte de Philips para su actualización.
- Para la vulnerabilidad sobre la versión 3.1 y anteriores y Xcelera versiones 4.1 y anteriores, se espera para octubre del 2018 una actualización que la resuelva.
- Como medida de mitigación mientras la nueva versión 3.2 pueda ser aplicada, Philips recomienda a los usuarios:
  - Revisar las políticas de accesos y permisos sobre los ficheros, restringiendo en la medida de lo posible dichos permisos.

Detalle:

- Gestión de privilegios inapropiada: En ISCV versión 2.X y anteriores y Xcelera 4.X y 3.X y anteriores, los servidores contienen una serie de servicios cuyos ejecutables son accesibles por un usuario autenticado y son arrancados con permisos elevados. Si un atacante local autenticado reemplazara uno de estos ejecutables por un programa malicioso, este también se ejecutaría con privilegios elevados. Se ha reservado el identificador CVE-2018-14787 para esta vulnerabilidad.
- Ausencia de comillas en un elemento o directorio de búsqueda: En ISCV versiones 3.X y anteriores y Xcelera 4.X y anteriores, existen una serie de servicios Windows corriendo con privilegios elevados, estos servicios no disponen de comillas en su definición de directorio, lo que permite a un posible atacante reemplazar estos servicios por otros ejecutables. Se ha reservado el identificador CVE-2018-14789 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en cardiógrafos PageWriter de Philips

Fecha de publicación: 17/08/2018

Importancia: Media

Recursos afectados:

- PageWriter TC10, TC20, TC30, TC50, TC70 todas las versiones anteriores a mayo de 2018.

Descripción:

Philips ha reportado varias vulnerabilidades de tipo validación incorrecta de los datos de entrada y uso de contraseñas embebidas en sus cardiógrafos PageWriter. Una explotación exitosa de estas vulnerabilidades podría dar lugar a desbordamientos de búfer o a permitir a un atacante acceder y modificar ajustes en el dispositivo.

Solución:

Philips tiene planeada una actualización para corregir estas vulnerabilidades a mediados de 2019.

Philips también ha proporcionado la siguiente información con respecto a un sistema operativo que ya no está respaldado por el fabricante:

- WinCE5 es un sistema operativo obsoleto, el cual ya no se encuentra respaldado por el fabricante y solo aplica a PageWriter TC20, TC30, TC50 y TC70.
- PageWriter TC50 y TC70 soportan WinCE7 que se encuentra disponible en el InCenter del cliente. Philips recomienda sustituir los dispositivos TC20 y TC30 por el TC50 si están preocupados por el sistema operativo obsoleto. Para el dispositivo TC20 se lanzará una actualización a finales de 2019 para actualizarlo a un sistema operativo compatible.

Detalle:

- El dispositivo PageWriter no realiza ninguna validación de los datos introducidos por el usuario. Esto puede dar lugar a vulnerabilidades de desbordamiento de búfer o ataques de formato de string. Se ha asignado el CVE-2018-14799 para esta vulnerabilidad.
- Un atacante que descubra la contraseña embebida de superusuario y acceso físico, puede utilizarla para acceder y modificar todas las configuraciones en el dispositivo, así como reestablecer las contraseñas existentes. Se ha asignado el identificador CVE-2018-14801 para esta vulnerabilidad.

Etiquetas: Sistema Operativo, Vulnerabilidad

Múltiples vulnerabilidades en productos Yokogawa

Fecha de publicación: 17/08/2018

Importancia: Alta

Recursos afectados:

- iDefine para ProSafe-RS versión R1.16.3 y anteriores.
- STARDOM en sus versiones VDS R7.50 y anteriores y FCN/FCJ Simulator R4.20 y anteriores.
- ASTPLANNER versión R15.01 y anteriores.
- TriFellows versión V5.04 y anteriores.
- Switches de capa 3 y capa 2 de Yokogawa en sus modelos:
  - GRVSW-663FA, GRVSW-664FA, GRVSW-665FA, GRVSW-666FA, GRVSW-667FA, GRVSW-660FA, GRVSW-661FA, GRVSW-662FA, GRVSW-668FA, GRVSW-669FA, GRVSW-670FA, GRVSW-671FA, GRVSW-672FA, GRVSW-673FA,
- Los Switches de capa 3 y capa 2 de Hirschmann también son afectados en sus modelos:
  - MACH104-20TX-F, MACH104-20TX-FR, MAR1040-4C4C4C4C9999EM9HPY, MAR1040-4C4C4C4C9999EMMHPYY, MAR1040-4C4C4C4C9999ELLHPYY, RS40-0009CCCCEDBPYY, MACH102-8TP-F, MACH102-24TP-F, MAR1040-4C4C4C4C9999EM9HRY1, MAR1040-4C4C4C4C9999EMMHRY1, MAR1040-4C4C4C4C9999ELLHRY1, MAR1040-4C4C4C4C9999EM9HRY2, MAR1040-4C4C4C4C9999EMMHRY2, MAR1040-4C4C4C4C9999ELLHRY2.

Descripción:

El fabricante Yokogawa ha reportado varias vulnerabilidades en la función de gestión de licencias y en varios switches de capa 2 y capa 3. Un atacante remoto puede aprovechar las mismas para ejecutar código arbitrario o provocar una denegación de servicio.

Solución:

Yokogawa dispone de nuevas versiones, que solucionan las vulnerabilidades para los productos:

- iDefine para ProSafe-RS versión R1.16.4
- STARTDOM VDS R8.10
- ASTPLANNER R15.02.01
- TriFellows V5.10

Para los Switches de capa 2 y capa 3, el fabricante recomienda desactivar el comando de debug tcpdump, ya que no dispone de un nuevo firmware.

Para más información, ver el enlace de referencia o ponerse en contacto con el equipo de soporte del fabricante.

Detalle:

- La función de gestión de licencias de los productos Yokogawa afectados no está correctamente implementada, permitiendo a un atacante aprovecharse de paquetes especialmente diseñados para provocar un desbordamiento de búfer, causando la denegación de servicio o la ejecución remota de código.
- La función de debug en los switches Vnet/IP de capa 2 y capa 3 dispone de una vulnerabilidad en el comando tcpdump. Un atacante puede aprovecharla mientras se ejecuta en la consola de debug el comando tcpdump, para provocar una desconexión de las comunicaciones o interferir en estas.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en DeltaV DCS Workstations de Emerson

Fecha de publicación: 17/08/2018

Importancia: Crítica

Recursos afectados:

- DeltaV versiones v11.3.1, v12.3.1, v13.3.0, v13.3.1, R5

Descripción:

Younes Dragoni de Nozomi Networks, Ori Perez de CyberX y Emerson han reportado estas vulnerabilidades cuya explotación exitosa podría permitir a un atacante, la ejecución de código arbitrario o la inyección y propagación de malware entre estaciones de trabajo.

Solución:

Emerson recomienda a los usuarios aplicar los parches a los productos afectados. Los parches de software están disponibles para los usuarios con acceso al Portal de soporte de Guardian de Emerson en https://guardian.emersonprocess.com/. Emerson recomienda consultar el artículo Knowledge Base AK-1800- 0042 (DSN18003) para obtener más información.

Las vulnerabilidades CVE-2018-14797, CVE-2018-14795 y CVE-2018-14791 no pueden ser explotadas si se implementan medidas de lista blanca, ya que se evitaría que se sobrescribieran los archivos.

Para limitar la exposición a estas y otras vulnerabilidades, se recomienda implementar y configurar sistemas DeltaV y componentes relacionados como se describe en el Manual de seguridad de DeltaV, que está disponible en el Portal de soporte de Guardian de Emerson.

Detalle:

- Un archivo DLL especialmente diseñado se puede colocar en la ruta de búsqueda y cargarse como una DLL interna y válida, lo que puede permitir la ejecución de código arbitrario. Se ha asignado el identificador CVE-2018-14797 para esta vulnerabilidad.
- Una validación incorrecta de la ruta podría permitir a un atacante reemplazar ficheros ejecutables. Se ha asignado el identificador CVE-2018-14795 para esta vulnerabilidad.
- Los usuarios sin privilegios de administración son capaces de cambiar ejecutables y librerías en los productos afectados. Se ha asignado el identificador CVE-2018-14791 para esta vulnerabilidad.
- Un puerto de comunicación abierto podría ser explotado para la ejecución de código arbitrario. Se ha asignado el identificador CVE-2018-14793 para esta vulnerabilidad.

Etiquetas: Actualización, Malware, Vulnerabilidad

Múltiples vulnerabilidades en Niagara de Tridium

Fecha de publicación: 17/08/2018

Importancia: Alta

Recursos afectados:

- Niagara AX Framework versión 3.8 y anteriores
- Niagara 4 Framework versión 4.4 y anteriores

Descripción:

Johnathan Gains y Leet Cyber Security han reportado estas vulnerabilidades de tipo salto de directorio y autenticación incorrecta. La explotación exitosa de estas vulnerabilidades podría bloquear el dispositivo al que se accede y una condición de desbordamiento de búfer podría permitir la ejecución remota de código.

Solución:

Tridium recomienda seguir las siguientes medidas:

- Niagara AX v3.8: aplicar la actualización 4 (3.08.401)
- Niagara 4 Framework v4.4: aplicar la actualización 1 (4.4.92.2.1)

Para más información sobre las actualizaciones consultar el siguiente enlace:

https://www.tridium.com/~/media/tridium/library/documents/niagara_ax_38_update_4niagara_44_update_1.ashx?la=en

Detalle:

- Una vulnerabilidad de salto de directorio en los sistemas Tridium Niagara AX y Niagara 4 instalados en sistemas Microsoft Windows puede ser explotada aprovechando las credenciales de administrador válidas de la plataforma. Se ha asignado el identificador CVE-2017-16744 para esta vulnerabilidad.
- Un atacante puede iniciar sesión en la plataforma local de Niagara utilizando un nombre de cuenta deshabilitado y una contraseña en blanco, consiguiendo el atacante acceso de administrador al sistema Niagara. Se ha asignado el identificador CVE-2017-16748 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en router ESP-200 de Eltex

Fecha de publicación: 20/08/2018

Importancia: Alta

Recursos afectados:

- Router ESP-200 versión 1.2.0

Descripción:

Alexander Nochvay y Andrey Muravitsky de Kaspersky Lab ICS-CERT han reportado estas vulnerabilidades del tipo inyección de comandos, configuraciones inseguras, contraseñas por defecto y divulgación de información. Una explotación exitosa de estas vulnerabilidades podría permitir a un atacante realizar una escalada de privilegios, la ejecución de código arbitrario, la ampliación de la superficie de ataque o la divulgación de información.

Solución:

- Se recomienda actualizar a la versión de firmware 1.3.0

Detalle:

- Mediante el uso de contraseñas por defecto, un atacante sin autenticación podría iniciar una sesión de administrador en el dispositivo. Se ha asignado el identificador CVE-2018-15360 para esta vulnerabilidad.
- Un atacante autenticado con privilegios bajos podría utilizar una configuración insegura de sudo para ampliar la superficie de ataque. Se ha asignado el identificador CVE-2018-15359 para esta vulnerabilidad.
- Un atacante autenticado con privilegios bajos podría activar un usuario con privilegios altos y utilizarlo para ampliar la superficie de ataque. Se ha asignado el identificador CVE-2018-15358 para esta vulnerabilidad.
- Un atacante autenticado con privilegios bajos podría extraer información del hash donde se incluye la contraseña de cada usuario. Se ha asignado el identificador CVE-2018-15357 para esta vulnerabilidad.
- Un atacante autenticado podría ejecutar código arbitrario mediante la inyección de comandos. Se ha asignado el identificador CVE-2018-15356 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en router Kraftway-24F2XG de Kraftway

Fecha de publicación: 20/08/2018

Importancia: Crítica

Recursos afectados:

- Kraftway-24F2XG, versión de firmware 3.5.30.1118

Descripción:

Los investigadores de seguridad Alexander Nochvay y Andrey Muravitsky de Kaspersky Lab ICS CERT han reportado vulnerabilidades del tipo denegación de servicio, cifrado SSL débil, desbordamiento de búfer y credenciales por defecto. Gracias a estas vulnerabilidades, un atacante remoto podría originar la denegación del servicio, obtener privilegios para acceder al router, ejecutar código malicioso de forma remota o descifrar la información intercambiada.

Solución:

- Se recomienda actualizar a la versión de firmware 3.5.47-315-gef7 y superiores.

Detalle:

- Un atacante remoto no autenticado en el dispositivo afectado, puede obtener privilegios de administrador utilizando credenciales por defecto para acceder al router. Se ha asignado el identificador CVE-2018-15350 para esta vulnerabilidad.
- Un atacante remoto podría crear un enlace malicioso y enviarlo a un usuario (víctima) con privilegios dentro del router afectado para originar una denegación de servicio. Se ha asignado el identificador CVE-2018-15351 para esta vulnerabilidad.
- Un atacante remoto con pocos privilegios podría originar una denegación de servicio en el dispositivo afectado. Se ha asignado el identificador CVE-2018-15352 para esta vulnerabilidad.
- La interfaz web posee dos vulnerabilidades de desbordamiento de búfer gracias a la cual un atacante podría originar una denegación de servicio o ejecutar código remoto. Se han asignado los identificadores CVE-2018-15353 y CVE-2018-15354 para estas vulnerabilidades.
- Las versiones 2 y 3 de SSL contienen debilidades relacionadas con la robustez del cifrado que poseen las comunicaciones. Un atacante podría aprovechar esta vulnerabilidad para descifrar la información intercambiada mediante el uso de técnicas de ataque como Man-in-the-Middle. Se ha asignado el identificador CVE-2018-15355 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Privacidad, Vulnerabilidad

Consumo descontrolado de recursos en IntelliVue Information Center iX de Philips

Fecha de publicación: 22/08/2018

Importancia: Media

Recursos afectados:

- Philips IntelliVue Information Center iX versión B.02

Descripción:

Un usuario anónimo ha reportado esta vulnerabilidad de tipo consumo descontrolado de recursos cuya explotación exitosa podría dar lugar a una condición de denegación de servicio y el sistema operativo dejaría de responder debido al ataque de red, lo que afectaría a la capacidad de las aplicaciones para cumplir con el uso previsto.

Solución:

- Philips ha identificado y aplicado mitigaciones para reducir el riesgo de explotación de esta vulnerabilidad. Para que los usuarios de

los dispositivos afectados mitiguen la exposición a esta vulnerabilidad, la compañía recomienda seguir las instrucciones de uso y las guías de servicio, que proporcionan controles de compensación, hasta la salida del parche a finales de septiembre de 2018.

Detalle:

- Un atacante podría comprometer la disponibilidad del dispositivo realizando el envío de múltiples peticiones UDP iniciales. Se ha asignado el identificador CVE-1999-0103 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Autenticación inapropiada en Alaris Plus de Becton, Dickinson and Company (BD)

Fecha de publicación: 24/08/2018

Importancia: Crítica

Recursos afectados:

Las siguientes versiones de bombas de jeringa médica Alaris Plus, versiones 2.3.6 y anteriores, se ven afectadas:

- Alaris GS
- Alaris GH
- Alaris CC
- Alaris TIVA

Descripción:

El investigador Elad Luz de CyberMDX ha reportado la vulnerabilidad al fabricante BD que posteriormente se ha puesto en contacto con el ICS-CERT (NCICC). La vulnerabilidad relacionada con la autenticación inapropiada, permitiría a un atacante acceder sin autorización al dispositivo, interfiriendo en su operativa cuando esté conectado a un servidor vía puerto serie.

Solución:

El fabricante ha informado que la vulnerabilidad no puede explotarse si el dispositivo está conectado a una estación de trabajo Alaris Gateway. Además, el atacante no podría acceder de forma remota al dispositivo, ni a PHI o PII mediante la explotación de la misma.

BD recomienda seguir las siguientes mitigaciones y medidas de control compensatorias para reducir el riesgo asociado a esta vulnerabilidad:

- El ataque utiliza una vulnerabilidad conocida en los terminales de los servidores. Los usuarios que utilicen estos terminales, deben entender que el uso de los terminales de los servidores no es compatible.
- Los usuarios deben asegurarse de que están operando con los dispositivos afectados en un entorno de red segmentado o con un dispositivo totalmente aislado a cualquier red sin ningún tipo de comunicaciones que interfieran en su operativa.
- Los usuarios deben utilizar conexiones a través de la estación de trabajo Alaris Gateway. Esta situación, desactivaría la función de control remoto evitando la explotación de la vulnerabilidad.

Detalle:

- incorrecta autenticación para las funcionalidades que requieren la identificación de usuarios. Se ha asignado el identificador CVE-2018-14786 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Vulnerabilidad de Cross Site Scripting en PowerLogic PM5560 de Schneider Electric

Fecha de publicación: 24/08/2018

Importancia: Alta

Recursos afectados:

- PM5560 versiones de firmware anteriores a 2.5.4

Descripción:

Ezequiel Fernandez y Bertin Jose han reportado esta vulnerabilidad de cross protocol inyection en el servidor web embebido del producto PowerLogic PM5560 que podría permitir la ejecución de código javascript.

Solución:

- Aplicar la siguiente actualización https://www.schneider-electric.com/en/download/document/PM5560_PM5563_V2.5.4_Release/

Detalle:

- El servidor web embebido del producto PowerLogic PM5560 es susceptible a un ataque de cross site scripting. Un atacante remoto podría explotar esta vulnerabilidad, manipulando los datos de entrada vía web, para causar la ejecución de código javascript. Se ha asignado el identificador CVE-2018-7795 para esta vulnerabilidad.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Comprobación inadecuada de condiciones inusuales en Modicon M221 de Schneider Electric

Fecha de publicación: 27/08/2018

Importancia: Media

Recursos afectados:

- Modicon M221, todas las versiones anteriores al firmware V1.6.2.0

Descripción:

Yehonatan Kfir de Radiflow ha informado a Schneider Electric sobre una vulnerabilidad de comprobación inadecuada de condiciones excepcionales o inusuales que afecta a los productos Modicon M221. Un potencial atacante remoto podría reiniciar los dispositivos afectados.

Solución:

Schneider Electric ha desarrollado un parche para esta vulnerabilidad implementado en la versión de firmware V1.6.2.0, que se distribuye con SoMachine Basic V1.6 SP2. Puede descargarse en el siguiente enlace: https://www.schneider-electric.com/en/download/document/SoMachineBasicV1.6SP2/

Detalle:

Un potencial atacante remoto podría enviar tramas de protocolo de programación malformadas que provoquen un reinicio en los dispositivos afectados debido a una inadecuada comprobación de condiciones excepcionales o inusuales. Se ha reservado el identificador CVE-2018-7789 para esta vulnerabilidad.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Evasión de autenticación en productos i.LON 600 de Echelon

Fecha de publicación: 28/08/2018

Importancia: Baja

Recursos afectados:

- Todos los productos i.LON 600

Descripción:

El investigador independiente Maxim Rupp ha reportado esta vulnerabilidad de tipo evasión de autenticación en los productos i.LON 600 de Echelon. Un atacante remoto podría evadir la autenticación y leer información de configuración y estadísticas de rendimiento.

Solución:

- Para minimizar la exposición a amenazas, Echelon recomienda instalar los dispositivos i.LON 600 y cualquier servidor que haga uso de ellos detrás de un cortafuegos o en una VLAN sin otros dispositivos. Utilizando VLAN se limita el vector de amenaza de otros dispositivos internos y usuarios que no son parte del mismo sistema que el i.LON 600 y los servidores asociados. Cuando se haga uso de un cortafuegos, y para minimizar la exposición a amenazas, Echelon recomienda que este no haga ningún reenvío de puertos al i.LON 600

Detalle:

- La autenticación en el i.LON 600 está controlada por las directivas de configuración en el archivo WebParams.dat. Al especificar que un conjunto particular de archivos o directorios no debería ser accesible sin autenticación, la ruta se coloca en el archivo de configuración como una cadena, pudiendo contener caracteres comodín opcionales (*) para hacer coincidir cero o más caracteres. Cuando se realiza una solicitud web, el URI debe coincidir con toda la ruta proporcionada, o no se requerirá autenticación. Al enviar peticiones web con barras superpuestas en el URI (por ejemplo, ?/forms/////Echelon/SetupSecurity.htm?), la ruta no coincidirá con la configurada para requerir autenticación y se podrá acceder a ella sin ningún nombre de usuario o contraseña.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en Modicon M221 de Schneider Electric

Fecha de publicación: 29/08/2018

Importancia: Alta

Recursos afectados:

- Modicon M221, todas las versiones anteriores a la V1.6.2.0

Descripción:

Los investigadores Irfan Ahmed, Hyunguk Yoo, Sushma Kalle y Nehal Ameen de la Universidad de Nueva Orleans, han reportado varias vulnerabilidades de tipo error en la gestión de información y de incorrecta gestión de permisos, privilegios y control de acceso, que afectan a los productos Modicon M221 de Schneider Electric. Un potencial atacante remoto podría reescribir contraseñas, decodificaarlas o

reenviar la secuencia de autenticación.

Solución:

- Schneider Electric ha desarrollado un parche para esta vulnerabilidad implementado en la versión de firmware V1.6.2.0, que se distribuye con SoMachine Basic V1.6 SP2. Puede descargarse en el siguiente enlace: https://www.schneider-electric.com/en/download/document/SoMachineBasicV1.6SP2/

Detalle:

- Vulnerabilidad que permite a un usuario no autorizado reenviar secuencias de autenticación. Un potencial atacante podría conectarse al producto afectado consiguiendo subir el programa original del PLC. Se ha reservado el identificador CVE-2018-7790 para esta vulnerabilidad.
- Vulnerabilidad que permite a usuarios no autorizados sobrescribir la contraseña original. Un potencial atacante podría conseguir subir el programa original del PLC. Se ha reservado el identificador CVE-2018-7791 para esta vulnerabilidad.
- Vulnerabilidad que permite a usuarios no autorizados decodificar las contraseñas utilizando tablas rainbow. Se ha reservado el identificador CVE-2018-7792 para esta vulnerabilidad.

Etiquetas: Schneider Electric, Vulnerabilidad

Debilidad del código en Capsule Datacaptor Terminal Server de Qualcomm Life

Fecha de publicación: 29/08/2018

Importancia: Crítica

Recursos afectados:

Las siguientes versiones de Capsule Datacaptor Terminal Server (DTS), que forman parte de un sistema de información de un dispositivo médico, se encuentran afectadas:

- Todas las versiones de Capsule DTS incluidas en el servidor web embebido Allegro RomPager desde la 4.01 a la 4.34.

Descripción:

Elad Luz de CyberMDX ha reportado esta vulnerabilidad de tipo debilidad del código. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto le ejecución de código sin autorización para obtener privilegios de administrador en el dispositivo.

Solución:

Capsule Technologies ha lanzado una actualización de firmware que soluciona esta vulnerabilidad en la versión Single Board del DTS, lanzado originalmente en 2009. Capsule Technologies insta encarecidamente a todos los usuarios con una versión Single Board del DTS a descargar el firmware desde el portal de cliente de Capsule y aplicarlo a los dispositivos afectados siguiendo el procedimiento de parcheo. El acceso al portal del cliente se puede encontrar en la siguiente ubicación:
https://customers.capsuletech.com/

Debido a limitaciones técnicas, la actualización de firmware solo soluciona la vulnerabilidad en las versiones Single Board y no la soluciona en estas otras versiones:

- Dual Board
- Capsule Digi Connect ES converted to DTS
- Capsule Digi Connect

Capsule recomienda a los usuarios con cualquiera de estas tres versiones de DTS, deshabilitar el servidor web embebido para mitigar esta vulnerabilidad. El servidor web solo se utiliza para la configuración durante la implantación inicial y no es necesario para el soporte remoto continuo del dispositivo.

Detalle:

Esta vulnerabilidad permitiría a un atacante enviar una cookie HTTP al portal de administración web para escribir datos arbitrarios en la memoria del dispositivo, lo que podría habilitar la ejecución de código remoto. Se ha asignado el identificador CVE-2014-9222 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en e-Alert Unit de Philips

Fecha de publicación: 31/08/2018

Importancia: Crítica

Recursos afectados:

- Philips e-Alert versión R2.1 y anteriores

Descripción:

Philips ha identificado varias vulnerabilidades, cuya explotación exitosa por parte de un atacante dentro de la misma subred, podría afectar o comprometer detalles de contacto de usuario y la integridad y/o la disponibilidad de los productos afectados. Estas vulnerabilidades podrían permitir a un atacante introducir datos de entrada inesperados en la aplicación, ejecutar código arbitrario, obtener información de la unidad o provocar que las unidades afectadas dejen de funcionar.

Solución:

En junio de 2018 Philips lanzó la versión R2.1 la cual solucionaba algunas de estas vulnerabilidades. Para el resto de vulnerabilidades, Philips tiene planeada otra actualización de software para finales del 2018.

Philips comunicará las opciones de servicio a todos los usuarios afectados y recomienda visitar el sitio web de seguridad que poseen sus productos para obtener la última información de seguridad publicada sobre este asunto y para otros productos de Philips. La información se encuentra disponible en el siguiente enlace:
https://www.philips.com/productsecurity
Como una mitigación inmediata de las vulnerabilidades en la LAN hasta que se pueda aplicar la actualización, Philips recomienda a los usuarios:

- Asegurar la implementación de buenas prácticas de seguridad de red.
- Limitar el acceso a la red de e-Alert de acuerdo con la documentación del producto.

Los usuarios con preguntas sobre sus instalaciones específicas de e-Alert deben ponerse en contacto con su equipo de soporte de servicio local de Philips o con su servicio regional de soporte e-Alert. La información de contacto está disponible en la siguiente ubicación:

https://www.usa.philips.com/healthcare/solutions/customer-service-solutions

Detalle:

- Validación incorrecta de los datos de entrada: el software no realiza una validación correcta de los datos de entrada, permitiendo al atacante proporcionar datos de entrada de una forma que no es esperada por el resto de la aplicación. Esto llevaría a que partes de la unidad reciban una entrada involuntaria, lo que puede resultar en un flujo de control alterado, control arbitrario de un recurso o ejecución de código arbitrario. Se ha asignado el identificador CVE-2018-8850 para esta vulnerabilidad.
- Cross Site Scripting (XSS): el software no realiza un correcto filtrado de los parámetros de entrada. Este hecho permitiría a un atacante ejecutar código en el lado del cliente cuando una víctima acceda al servidor web mediante su navegador. Se ha asignado el identificador CVE-2018-8846 para esta vulnerabilidad.
- Permisos por defecto incorrectos: el software, al momento de la instalación, establece permisos incorrectos para un objeto que lo expone a un usuario no deseado. Se ha asignado el identificador CVE-2018-8848 para esta vulnerabilidad.
- Transmisión de información sensible en texto claro: el software transmite información sensible o de seguridad crítica en texto en claro en un canal de comunicación que puede ser capturado por un atacante. El canal de comunicación del producto no está cifrado lo que podría dar lugar a la divulgación de la información de contacto personal y de las credenciales de inicio de sesión de la aplicación dentro de la misma subred. Se ha asignado el identificador CVE-2018-8842 para esta vulnerabilidad.
- Consumo de recursos descontrolado: el software no restringe adecuadamente el tamaño o la cantidad de recursos solicitados por un usuario, lo cual puede utilizarse para consumir más recursos de los previstos. Se ha asignado el identificador CVE-2018-8854 para esta vulnerabilidad.
- Uso de contraseñas embebidas: el software contiene embebida la llave criptográfica que se usa para el cifrado de datos internos. Se ha asignado el identificador CVE-2018-8856 para esta vulnerabilidad.

Además de estas vulnerabilidades, también se han identificado otras de menor criticidad, para las que se han reservado los siguientes identificadores: CVE-2018-14803, CVE-2018-8844, CVE-2018-8852.

Etiquetas: Vulnerabilidad