Boletín de Junio de 2018

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en MDS PulseNET de GE

Fecha de publicación: 01/06/2018

Importancia: Alta

Recursos afectados:

- MDS PulseNET versión 3.2.1 y anteriores
- MDS PulseNET Enterprise versión 3.2.1 y anteriores

Descripción:

El investigador rgod ha reportado varias vulnerabilidades a Zero Day Initiative (ZDI) de tipo autenticación incorrecta, restricción inadecuada de referencia XML de entidad externa y ruta transversal relativa que afectan a MDS PulseNET y MDS PulseNET Enterprise de GE. Un potencial atacante podría conseguir una elevación de privilegios o exfiltración de información mediante estas vulnerabilidades.

Solución:

GE ha modificado el software y la arquitectura del producto PulseNET. La última versión soluciona estas vulnerabilidades. GE anima a sus usuarios a actualizar PulseNET a la versión 4.1 o posterior para eliminar estas vulnerabilidades.

Las actualizaciones disponibles para PulseNET estÃin disponibles en:

http://www.gegridsolutions.com/Communications/MDS/PulseNET_Download.aspx

Las actualizaciones disponibles para PulseNET Enterprise estÃin disponibles en:

http://www.gegridsolutions.com/Communications/MDS/PulseNETEnt_Download.aspx

Detalle:

- Autenticación incorrecta: un potencial atacante no autorizado podría aprovechar el puerto de entrada de Java Remote Proper Invocation (RMI) para lanzar aplicaciones y dar soporte a la ejecución de código remoto a través de servicios Web. Se ha asignado el identificador CVE-2018-10611 para esta vulnerabilidad.
- Restricción inadecuada de referencia XML de entidad externa: un potencial atacante podría utilizar múltiples variantes de ataques XML External Entity (XXE) para exfiltrar datos de la plataforma Windows. Se ha asignado el identificador CVE-2018-10613 a esta vulnerabilidad.
- Salto de ruta relativa: un potencial atacante podría aprovechar un salto de directorio para producir una exfiltración o borrado de ficheros en la plataforma. Se ha asignado el identificador CVE-2018-10615 a esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Delta Industrial Automation DOPSoft de Delta Electronics

Fecha de publicación: 01/06/2018

Importancia: Alta

Recursos afectados:

- DOPSoft versión 4.00.04 y anteriores.

Descripción:

El investigador B0nd @garagehackers, trabajando con Zero Day Initiative de Trend Micro, ha identificado varias vulnerabilidades de tipo

desbordamiento de búfer y lectura fuera de límites en el producto Delta Industrial Automation DOPSoft de Delta Electronics. Un potencial atacante remoto podría leer información confidencial, ejecutar código arbitrario y/o provocar una caída de la aplicación.

Solución:

Delta Electronics recomienda a los usuarios afectados actualizar a la última versión disponible aquí:

http://www.deltaww.com/Products/PluginWebUserControl/downloadCenterCounter.aspx?DID=9063&DocPath=1&hl=en-US

Delta Electronics recomienda también a los usuarios afectados restringir la interacción con la aplicación a ficheros de confianza.

Detalle:

- **Lectura fuera de límites**: La aplicación implementa operaciones de lectura de un búfer de memoria donde la posición puede ser determinada mediante un valor leído de un fichero .dpa. Esto puede causar una restricción inadecuada de las operaciones dentro de los límites del búfer de memoria, permitir la ejecución de código remoto, alterar el flujo de control previsto, permitir la lectura de información confidencial o provocar una caída de la aplicación. Se ha asignado el identificador CVE-2018-10623 para esta vulnerabilidad.
- **Desbordamiento de búfer**: La aplicación utiliza un búfer de longitud fija donde un valor mayor que la longitud del búfer de pila se puede leer desde un archivo .dpa, haciendo que el búfer se sobrescriba. Esto podría permitir ejecución remota de código y provocar una caída de la aplicación. Se han asignado los identificadores CVE-2018-10617 y CVE-2018-10621 para estas vulnerabilidades.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en U.motion Builder de Schneider Electric

Fecha de publicación: 04/06/2018

Importancia: Crítica

Recursos afectados:

- U.motion Builder todas las versiones anteriores a la versión 1.3.4

Descripción:

 y Wei Gao (Ixia A Keysight Business) han reportado a Schneider Electric una serie de vulnerabilidades cuya explotación podría permitir a un atacante la ejecución de código arbitrario, leer el búfer de memoria, causar un fallo de segmentación o evadir la autenticación.

Solución:

Schneider Electric ha publicado la versión 1.3.4 que soluciona estas vulnerabilidades y estÃ¡ disponible en:

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

Detalle:

Las vulnerabilidades identificadas son:

- Falta de validación de los datos de entrada: Esta vulnerabilidad ocurre cuando los datos de entrada son evaluados como un comando por la aplicación. De esta manera, un atacante podría ejecutar código arbitrario, leer el búfer de memoria o causar un fallo de segmentación en la aplicación. Se ha asignado el identificador CVE-2018-7784 para esta vulnerabilidad de severidad crítica.
- Evasión de autenticación: Una inyección de comando remoto permite la evasión de la autenticación. Se ha asignado el identificador CVE-2018-7785 para esta vulnerabilidad de severidad crítica.
- Cross-Site-Scripting (?XSS?): Existe una vulnerabilidad de Cross-Site-Scripting (?XSS?) que podría permitir a un atacante la inyección de scripts maliciosos. Se ha asignado el identificador CVE-2018-7786 para esta vulnerabilidad de severidad media.
- Validación inadecuada de datos de entrada: Esta vulnerabilidad se debe a una validación inadecuada de los datos de entrada en una petición HTTP GET. Se ha asignado el identificador CVE-2018-7787 para esta vulnerabilidad de severidad media.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Múltiples vulnerabilidades en IntelliVue Patient Monitors y Avalon Fetal/Maternal Monitors de Philips

Fecha de publicación: 06/06/2018

Importancia: Alta

Recursos afectados:

- IntelliVue Patient Monitors MP Series (MP2/ X2/ MP30/ MP50/ MP70/ NP90/ MX700/ 800) Rev B-M
- IntelliVue Patient Monitors MX (MX400-550) Rev J-M y (X3/MX100 solo Rev M)
- Avalon Fetal/Maternal Monitors FM20/FM30/FM40/FM50 Revisiones F.0, G.0 y J.3

Descripción:

Oran Avraham de Medigate, en coordinación con Philips, ha reportado estas vulnerabilidades a NCCIC. Una explotación exitosa de estas vulnerabilidades podría permitir a un atacante leer/escribir memoria y/o provocar una denegación de servicio a través de un reinicio del sistema, lo que puede dar lugar a un retraso en el diagnóstico y tratamiento de los pacientes.

Solución:

Philips proporcionarÃi un parche de corrección para versiones específicas, así como una actualización para todas las versiones.

Philips ofrece las siguientes mitigaciones para estas vulnerabilidades:

- Philips recomienda seguir las instrucciones del dispositivo afectado. Philips proporcionarÃi soluciones para IntelliVue revisiones J-M y Avalon revisiones G.0 y J.3 en 2018 en forma de parche. Para aquellos usuarios con versiones mÃis antiguas de IntelliVue, Philips proporcionarÃi una ruta de actualización para las revisiones soportadas. Para las opciones de actualización, los usuarios deben comunicarse con su representante de ventas de Philips.
- En el caso de IntelliVue Monitors, Philips recomienda a los usuarios que sigan las instrucciones de uso (Seguridad para la Guía de redes clínicas) de seguridad física y lógica. Adicionalmente, Philips recomienda a los usuarios actualizar a la revisión K.2 o posterior.
- Para Avalon Fetal Monitor versiones G.0 y J.3 Philips recomienda a los usuarios seguir el manual de instalación y servicio (Privacidad de Datos y Requisitos de Seguridad de Red).
- Para Avalon Fetal Monitor F.0 Philips recomienda a los usuarios que sigan las instrucciones tal como se documenta en la sección Rev J.3 Guía de servicios Privacidad de datos y Requisitos de seguridad de la red.
- Para los usuarios con preguntas sobre sus instalaciones específicas de IntelliVue y Avalon Fetal Monitor Philips recomienda ponerse en contacto con su equipo de soporte de servicio local de Philips o con su servicio de soporte regional.

Detalle:

- Autenticación incorrecta: Esta vulnerabilidad permite a un atacante sin autorización acceder a la memoria desde una dirección de dispositivo elegida por el atacante dentro de la misma subred. Se ha asignado el identificador CVE-2018-10597 para esta vulnerabilidad de severidad alta.
- Exposición de la información: Esta vulnerabilidad permite a un atacante sin autorización leer memoria desde una dirección de dispositivo elegida por el atacante dentro de la misma subred. Se ha asignado el identificador CVE-2018-10599 para esta vulnerabilidad de severidad media.
- Desbordamiento de búfer basado en la pila: Esta vulnerabilidad expone un servicio de ?echo?, en el que un búfer enviado por un atacante a una dirección de dispositivo elegida por el atacante dentro de la misma subred se copia a la pila sin verificaciones de límites, dando lugar a un desbordamiento de pila. Se ha asignado el identificador CVE-2018-10601 para esta vulnerabilidad de severidad alta.

Etiquetas: Vulnerabilidad

Vulnerabilidad en RSLinx Classic y FactoryTalk Linx Gateway de Rockwell Automation

Fecha de publicación: 08/06/2018

Importancia: Alta

Recursos afectados:

- RSLinx Classic versión 3.90.01 y anteriores.
- FactoryTalk Linx Gateway versión 3.90.00 y anteriores.

Descripción:

Gjoko Krstic de Zero Science Lab, junto con Rockwell Automation, ha reportado esta vulnerabilidad a NCCIC que podría permitir a un usuario local, autorizado, pero sin privilegios, ejecutar código arbitrario y también el escalado de privilegios de usuario en la estación de trabajo afectada.

Solución:

- RSLinx Classic versión 3.90.01 y anteriores, actualizar a la versión 4.00.01 o posterior disponible en https://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?crumb=112
- FactoryTalk Linx Gateway vesión 3.90.00 y anteriores, actualizar a la versión 6.00.00 o posterior disponible en https://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?crumb=112

Detalle:

Una vulnerabilidad de elemento o ruta de búsqueda no entrecomillado podría permitir a un usuario local, autorizado, pero sin privilegios, ejecutar código arbitrario y también el escalado de privilegios de usuario en la estación de trabajo afectada. Se ha asignado el identificador CVE-2018-10619 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Siemens

Fecha de publicación: 13/06/2018

Importancia: Crítica

Recursos afectados:

- Sistemas RAPIDLab 1200, RAPIDPoint 400 y RAPIDPoint 500, todas las versiones que no utilicen productos Siemens Healthineers Informatics.
- RAPIDLab 1200 Series, todas las versiones anteriores a la 3.3 con los productos Siemens Healthineers Informatics.
- Sistemas RAPIDPoint 500: versiones 3.0 y posteriores, versión 2.4.X y versiones 2.3 y anteriores con los productos Siemens Healthineers Informatics.
- Sistemas RAPIDPoint 400: Todas las versiones con los productos Siemens Healthineers Informatics.
- RFID 181-EIP todas las versiones

- RUGGEDCOM WiMAX, versiones 4.4 y 4.5.
- SCALANCE X-200, versiones anteriores a la 5.2.3.
- SCALANCE X-200 IRT, versiones anteriores a la 5.4.1.
- SCALANCE X-204RNA, todas las versiones.
- SCALANCE X-300, todas las versiones.
- SCALANCE X408, todas las versiones.
- SCALANCE X414, todas las versiones.
- SIMATIC RF182C, todas las versiones
- SCALANCE X-200, versiones anteriores a la 5.2.3.
- SCALANCE X-200 IRT, versiones anteriores a la 5.4.1.
- SCALANCE X-300, todas las versiones.
- SCALANCE M875, todas las versiones.
- License Management System (LMS), versiones 2.1 y anteriores.
- Annual Shading versiones 1.0.4 y 1.1.
- Desigo AVT, versiones 3.1.0, 3.0.1 y anteriores (builds 12.10.318,12.0.850.0, 11.10.55.0, 11.0.360.0, 10.10.845.0 y 10.0.830.0).
- Desigo CC / Cerberus DMS, versiones 1.1, 2.0, 2.1 y 3.0.
- Desigo Configuration Manager (DCM), versiones 6.1 SP2 y anteriores, 6.0 SP1 y anteriores.
- Desigo XWP versiones 6.1 y anteriores.
- SiteIQ Analytics versiones 1.1, 1.2 y 1.3.
- Siveillance Identity versión 1.1

Descripción:

Se han identificado un total de 14 vulnerabilidades en productos Siemens, siendo 1 de ellas de severidad crítica, 8 altas y 5 medias.

Solución:

- Para los sistemas RAPIDLab 1200, RAPIDPoint 400 y RAPIDPoint 500, todas las versiones que no utilicen productos Siemens Healthineers Informatics.
  - Restringir el acceso físico a personal estrictamente autorizado.
  - Deshabilitar la característica ?Remote Viewing? siguiendo las instrucciones de la Guía de Operadores, sección ?Enabling or Disabling Remote Viewing?.
- Para RAPIDLab 1200 Series, todas las versiones anteriores a la 3.3 con los productos Siemens Healthineers Informatics:
  - Restringir el acceso físico a personal estrictamente autorizado.
  - Actualizar a la versión 3.3 o 3.3.1.
  - Modificar la contraseña.
  - Para garantizar una conectividad segura con RAPIDCommÂ® Data Management System, se recomienda utilizar RAPIDCommÂ® V7.0 o superior.
- Para los sistemas RAPIDPoint 500, versiones 3.0 y posteriores, versión 2.4.X y versiones 2.3 y anteriores con los productos Siemens Healthineers Informatics
  - Restringir el acceso físico a personal estrictamente autorizado.
  - Modificar la contraseña.
  - Para garantizar una conectividad segura con RAPIDComm, se recomienda utilizar RAPIDComm V7.0 o superior.
- Para todas las versiones de RAPIDPoint 400 con los productos Siemens Healthineers Informatics:
  - Restringir el acceso físico a personal estrictamente autorizado.
  - Actualizar a la serie RAPIDPoint 500.
  - Si la actualziación no es posible, se recomienda deshabilitar la característica ?Remote Viewing?, siguiendo las instrucciones de la Guía de Operadores sección ?Enabling or Disabling Remote Viewing?
- Para todas las versiones de los equipos RFID 181-EIP, SIMATIC RF182C y SCALANCE-X-204RNA, SCALANCE X-300, SCALANCE X408, SCALANCE X414, así como las versiones 4.4 y 4.5 de Ruggedcom Wimax:
  - Utilizar direcciones IP estÃiticas en lugar de DHCP.
  - Aplicar el concepto de protección de celda (p. ej. aplicar ?port security? en los switches).
  - Aplicar estrategias de defensa en profundidad
- Versiones inferiores a 5.2.3 del conmutador SCALANCE X-200:
  - Actualizar el firmware a la versión 5.2.3
- Versiones inferiores a 5.4.1 del conmutador SCALANCE X-200 IRT:
  - Actualizar el firmware a la versión 5.4.1
- Versiones inferiores a 5.2.3 del conmutador SCALANCE X-200:
  - Actualizar el firmware a la versión 5.2.3
- Versiones inferiores a 5.4.1 del conmutador SCALANCE X-200 IRT:
  - Actualizar el firmware a la versión 5.4.1
- Todas las versiones del conmutador SCALANCE X300:
  - Proteger el acceso de red a los dispositivos afectados.
- Todas las versiones de SCALANCE M875:
  - Actualizar hardware al modelo SCALANCE M876-4 o RUGGEDCOM RM1224.
  - Mientras no se actualice el firmware, también se recomienda restringir el acceso a la interfaz de gestión web únicamente a las redes internas o VPN, utilizar el cortafuegos de serie del producto para restringir el acceso a la interfaz web a direcciones IP confiables, proteger la cuenta de usuario administrativa con contraseñas robustas y no navegar por otras pÃiginas o hacer clic en enlaces externos mientras se esté autenticando a la interfaz web de administración.
- Para las versiones de License Management System (LMS) 2.1 y anteriores:
  - Actualizar el dongle driver siguiendo las indicaciones disponibles en la web de Siemens.
- Para las versiones de Annual shading 1.0.4 y 1.1:
  - Actualizar el dongle driver siguiendo las indicaciones disponibles en la web de Siemens.
- Para las versiones de Desigo AVT 3.1.0, 3.0.1 y anteriores (builds 12.10.318,12.0.850.0, 11.10.55.0, 11.0.360.0, 10.10.845.0 y 10.0.830.0):
  - Actualizar el dongle driver siguiendo las indicaciones disponibles en la web de Siemens.
- Para las versiones de Desigo CC / Cerberus DMS 1.1, 2.0, 2.1 y 3.0:
  - Actualizar el dongle driver siguiendo las indicaciones disponibles en la web de Siemens.
- Para las versiones de Desigo Configuration Manager (DCM) 6.1 SP2 y anteriores, 6.0 SP1 y anteriores:
  - Actualizar el dongle driver siguiendo las indicaciones disponibles en la web de Siemens.
- Para las versiones de Desigo XWP 6.1 y anteriores:
  - Actualizar el dongle driver siguiendo las indicaciones disponibles en la web de Siemens.
- Para las versiones de SiteIQ Analytics 1.1, 1.2 y 1.3:
  - Actualizar el dongle driver siguiendo las indicaciones disponibles en la web de Siemens.
- Para las versiones de Siveillance Identity 1.1:
  - Actualizar el dongle driver siguiendo las indicaciones disponibles en la web de Siemens.

Detalle:

- Atacantes remotos con credenciales de acceso locales o remotas a la característica ?Remote View?, podrían elevar sus privilegios, comprometiendo la confidencialidad, integridad y disponibilidad del sistema. Se ha reservado el identificador CVE- 2018-4845 para esta vulnerabilidad de severidad alta.
- Una cuenta de fÃibrica con la contraseña embebida podría permitir a los atacantes acceder al dispositivo a través del puerto TCP 5900, comprometiendo la confidencialidad, integridad y disponibilidad del sistema. Se ha reservado el identificador CVE- 2018-4846 para esta vulnerabilidad de severidad alta

- Un atacante remoto sin privilegios que se sitúe localmente en el mismo segmento de red que los dispositivos afectados podría ser capaz de ejecutar código de forma remota en ellos mediante el envío de respuestas DHCP, especialmente manipuladas ante peticiones DHCP de un cliente. Se ha reservado el identificador CVE-2018-4833 para esta vulnerabilidad de severidad alta.
- Un atacante remoto autenticado con acceso a la interfaz web (443/tcp) podría ejecutar arbitrariamente comandos del sistema operativo. Se han reservado los identificadores CVE-2018-4859 y CVE-2018-4860 para estas vulnerabilidades de severidad alta.
- La interfaz web del puerto 443/tcp podría permitir un ataque Cross-Site Request Forgery (CSRF) si un usuario desprevenido es engañado para acceder a un vínculo malicioso. Se ha reservado el identificador CVE-2018-11447 para esta vulnerabilidad de severidad alta.
- Un atacante no autenticado podría realizar una denegación de servicio (DoS) sin necesidad de interacción del usuario. Se ha reservado los identificadores CVE-2018-6304 y CVE-2018-6305 para esta vulnerabilidad de severidad alta.
- Un atacante no autenticado podría inyectar código en la pÃigina de logs de Admin Control Center. El código es ejecutado cuando un usuario administrador visita la pÃigina afectada pudiendo afectar a la confidencialidad, integridad y disponibilidad del sistema. Se ha reservado el identificador CVE-2018-8900 para esta vulnerabilidad de severidad crítica.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en Xltek NeuroWorks de Natus Medical

Fecha de publicación: 15/06/2018

Importancia: Crítica

Recursos afectados:

- Natus Xltek NeuroWorks Versión 8

Descripción:

Cory Duplantis, de Cisco Talos, ha descubierto y reportado estas vulnerabilidades a Natus. Para la explotación exitosa de estas vulnerabilidades se requiere acceso a la red de clientes de Natus, pudiendo bloquear el dispositivo al que se accede. Una condición de desbordamiento de búfer podría permitir la ejecución de código remoto.

Solución:

Natus ha publicado NeuroWorks/SleepWorks 8.5 GMA 3, una actualización de software con las mejoras de seguridad que solucionan estas vulnerabilidades identificadas en NeuroWorks/SleepWorks 8. La actualización estÃi disponible para los usuarios de NeuroWorks/SleepWorks 8.0, 8.1, 8.4 y 8.5. Póngase en contacto con el departamento de soporte técnico de Natus Neuro llamando al 1-800 387-7516 o envíe un correo electrónico a para obtener mÃis detalles.

Detalle:

- Un paquete especialmente diseñado, puede causar una lectura fuera de límites, lo que puede dar como resultado una condición de denegación de servicio. Se han reservado los identificadores CVE-2017-2852, CVE-2017-2858, CVE-2017-2860, CVE-2017-2861 para estas vulnerabilidades.
- Un atacante puede causar un desbordamiento de búfer enviando un paquete especialmente diseñado al producto afectado mientras el producto intenta abrir un archivo solicitado por el cliente. Se ha reservado el identificador CVE-2017-2853 para esta vulnerabilidad.
- Un paquete especialmente diseñado que se recibe durante la ejecución de ciertos comandos puede hacer que la memoria se sobrescriba de una manera que podría permitir que un atacante tome el control del programa. Se ha reservado el identificador CVE-2017-2867 para esta vulnerabilidad.
- Un error en la forma en que el programa analiza las estructuras de datos puede permitir que un atacante tome el control del sistema enviÃindole un paquete especialmente diseñado. Se ha reservado el identificador CVE-2017-2868 para esta vulnerabilidad.
- Un paquete especialmente diseñado puede aprovechar la forma en que el programa analiza las estructuras de datos y causar un desbordamiento de búfer, permitiendo la ejecución remota de código arbitrario. Se ha reservado el identificador CVE-2017-2869 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Secuestro de DLL en Pluto Manager de ABB

Fecha de publicación: 19/06/2018

Importancia: Media

Recursos afectados:

- Pluto Manager versiones 2.24-2.34.3

Descripción:

El investigador independiente Herman Groeneveld ha identificado una vulnerabilidad de secuestro de DLL en la aplicación Pluto Manager de ABB. Un potencial atacante local podría ejecutar código malicioso con los mismos privilegios que la aplicación.

Solución:

- ABB ha publicado la versión 2.36 de Pluto Manager de ABB que soluciona esta vulnerabilidad.

Detalle:

Un potencial atacante local podría renombrar una DLL maliciosa para que sea cargada por la aplicación, ya que no se realiza una verificación de la corrección de las DLL cargadas. Cuando la aplicación cargue la DLL, el código malicioso se ejecutaría con los mismos privilegios que la aplicación.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en cámaras de Axis Communications

Fecha de publicación: 20/06/2018

Importancia: Media

Recursos afectados:

Los equipos de investigación de seguridad de VDOO, han descubierto vulnerabilidades en 390 modelos de cÃimaras de Axis que han sido confirmadas por el fabricante.
Se puede comprobar la lista completa de productos afectados en el siguiente enlace: https://www.axis.com/files/sales/ACV-128401_Affected_Product_List.pdf

Descripción:

Investigadores de VDOO han encontrado varias vulnerabilidades que afectan a diferentes modelos de cÃimaras IP de la compañía Axis Communications. Un potencial atacante con acceso a la red podría aprovechar las vulnerabilidades y conseguir evadir la autenticación, enviar comandos sin restricciones, ejecutar código arbitrario o denegar el servicio en los productos afectados.

Solución:

Axis ha publicado nuevas versiones de firmware para los productos afectados que solucionan estas vulnerabilidades y recomienda actualizarlos a la mayor brevedad posible.

Las versiones de firmware asociadas con cada producto pueden comprobarse en el siguiente enlace:
https://www.axis.com/files/sales/ACV-128401_Affected_Product_List.pdf

Detalle:

Las vulnerabilidades identificadas son las siguientes:

- Evasión de autenticación: Un potencial atacante podría enviar una petición no autenticada que alcance la funcionalidad .srv de /bin/ssid y evadir el mecanismo de autenticación. Se ha reservado el identificador CVE-2018-10661 para esta vulnerabilidad.
- Acceso sin restricciones: La funcionalidad .srv permite seleccionar múltiples acciones. Un potencial atacante podría utilizar alguna de las acciones permitidas para ejecutarlas sin ningún tipo de restricción. Se ha reservado el identificador CVE-2018-10662 para esta vulnerabilidad.
- Ejecución de código arbitrario: El parÃimetro perhand permite la modificación de parÃimetros internos de los dispositivos. Un potencial atacante podría modificar las peticiones de cambio de parÃimetros para ejecutar diferentes acciones. Se ha reservado el identificador CVE-2018-10660 para esta vulnerabilidad.
- Denegación de servicio: Un potencial atacante podría utilizar una url especialmente malformada para detener la ejecución del proceso httpd y provocar una denegación de servicio. Se ha reservado el identificador CVE-2018-10664 para esta vulnerabilidad.
- Divulgación de información: Un potencial atacante no autenticado podría modificar los parÃimetros devueltos por el navegador para obtener un tamaño de información mayor del solicitado y obtener información protegida. Se ha reservado el identificador CVE-2018-10663 para esta vulnerabilidad.
- Denegación de servicio: Un potencial atacante no autenticado podría enviar un paquete mbus especialmente manipulado para detener el servicio ssid. Se ha reservado el identificador CVE-2018-10658 para esta vulnerabilidad.
- Denegación de servicio: Un potencial atacante no autenticado podría enviar un comando especialmente manipulado que llame a una instrucción ARM no definida para detener el servicio ssid. Se ha reservado el identificador CVE-2018-10659 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Desbordamiento de búfer en Delta Industrial Automation COMMGR de Delta Electronics

Fecha de publicación: 22/06/2018

Importancia: Alta

Recursos afectados:

- COMMGR, versión 1.08 y anteriores
  - DVPSimulator EH2, EH3, ES2, SE, SS2
  - AHSIM_5x0, AHSIM_5x1

Descripción:

Un investigador anónimo trabajando con Zero Day Initiative de Trend Micro ha identificado un desbordamiento de búfer que afecta al software de gestión de comunicaciones Delta Industrial Automation COMMGR de Delta Electronics. Un potencial atacante remoto podría llegar a ejecutar código remoto y causar que la aplicación falle o una denegación de servicio en el servidor de la aplicación.

Solución:

Delta Electronics ha publicado la versión v1.09 del software que soluciona esta vulnerabilidad. La versión puede encontrarse en el siguiente enlace: http://www.deltaww.com/Products/PluginWebUserControl/downloadCenterCounter.aspx?DID=2093&DocPath=1&hl=en-US

Delta Electronics también recomienda la aplicación de listas blancas para permitir solo las comunicaciones autorizadas sobre los puertos 502 y 10002.

Detalle:

La aplicación utiliza un búfer de longitud fija donde un valor de longitud no definida puede ser leído por los paquetes de red mediante un puerto de red específico, causando que el búfer se sobrescriba. Esto permite la ejecución remota de código, que la aplicación falle o una

denegación de servicio en el servidor de la aplicación. Se ha asignado el identificador CVE-2018-10594 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Validación incorrecta de campos de entrada en productos Rockwell Automation

Fecha de publicación: 22/06/2018

Importancia: Alta

Recursos afectados:

- Allen-Bradley CompactLogix 5370 L1, L2 y L3 versión 30.012 y anteriores.
- Allen-Bradley Armor CompactLogix 5370 L3 versión 30.012 y anteriores.
- Allen-Bradley Compact GuardLogix 5370 versión 30.012 y anteriores.
- Allen-Bradley Armor Compact GuardLogix 5370 versión 30.012 y anteriores.

Descripción:

Alexey Perepechko de Applied Risk ha identificado una vulnerabilidad de tipo validación incorrecta de campos de entrada que afecta a diferentes productos de Rockwell Automation y que podría causar una denegación de servicio.

Solución:

Rockwell Automation recomienda a los usuarios afectados actualizar a la revisión de firmware FRN (31.011 o posterior) en los productos afectados. El firmware se encuentra disponible en el siguiente enlace:
https://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?crumb=112

También recomienda implementar las siguientes medidas preventivas:

- Bloquear todo el trÃifico a Ethernet / IP u otros dispositivos basados en el protocolo CIP desde fuera de la zona de fabricación, bloqueando o restringiendo el acceso a los puertos 2222 y 44818 / TCP y UDP, utilizando la infraestructura de red apropiada, como firewalls, dispositivos UTM u otros dispositivos de seguridad. Para obtener mÃis información sobre los puertos TCP / UDP utilizados por Rockwell Automation Products, consulte el artículo ID 898270 de la base de conocimiento disponible en: https://rockwellautomation.custhelp.com/app/answers/detail/a_id/898270/page/1
- Minimizar la exposición de la red para todos los dispositivos y / o sistemas del sistema de control y asegurarse de que no sean accesibles desde Internet.
- Cuando se requiera acceso remoto, usar métodos seguros, como Redes Privadas Virtuales (VPN).

Detalle:

Un potencial atacante podría enviar un paquete TCP específico y causar un fallo importante no recuperable (MNRF), dando lugar a una denegación de servicio. Se ha asignado el identificador CVE-2017-9312 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de control de acceso en múltiples productos de Siemens

Fecha de publicación: 26/06/2018

Importancia: Media

Recursos afectados:

- IEC 61850 system configurator, todas las versiones anteriores a V5.80
- DIGSI 5, todas las versiones anteriores a V7.80
- DIGSI 4, todas las versiones
- SICAM PAS/PQS, todas las versiones anteriores a V8.11
- SICAM PQ Analyzer, todas las versiones anteriores a V3.11
- SICAM SCC todas las versiones

Descripción:

Chris Bellows y HD Moore de Atredis Partners y Austin Scott de San Diego Gas and Electric han reportado estas vulnerabilidades a Siemens. Los productos afectados por esta vulnerabilidad podrían permitir a un atacante filtrar limitados datos del sistema o la ejecución de código con permisos de usuario del sistema operativo.

Solución:

Siemens recomienda las siguientes medidas para cada producto afectado:

- IEC 61850 system configurator: Actualizar a la versión V5.80 disponible en https://support.industry.siemens.com/cs/ww/en/view/109740546
- DIGSI 5: Desinstalar IEC 61850 system configurator o actualizar a la versión V7.80 disponible en https://support.industry.siemens.com/cs/ww/en/view/109758531
- SICAM PAS/PQS: Actualizar a la versión V8.11 disponible en https://support.industry.siemens.com/cs/us/en/view/109757831
- SICAM PQ Analyzer: Actualizar a la versión V3.11 disponible en https://support.industry.siemens.com/cs/us/en/view/109757833
- DIGSI 4 y SICAM SCC: Cambiar la configuración del firewall para restringir el acceso a los puertos TCP 4884,5885 y 5886 a localhost (dependiendo del producto afectado). AdemÃis seguir las directrices de seguridad de subestaciones seguras disponibles en https://www.siemens.com/gridsecurity

Detalle:

Un servicio de los productos afectados que escucha en todas las interfaces de red del host en los puertos TCP 4884, 5885 y 5886 podría permitir a un atacante filtrar datos limitados del sistema o ejecutar código con permisos de usuario de Microsoft Windows.

Una explotación exitosa requiere que un atacante pueda enviar una solicitud de red especialmente diseñada al servicio vulnerable y que un usuario interactúe con la aplicación cliente del servicio en el anfitrión. Para ejecutar código arbitrario con permisos de usuario de Microsoft Windows, un atacante debe ser capaz de implantar el código de antemano en el anfitrión por otros medios. Se ha reservado el identificador CVE-2018-4858 para esta vulnerabilidad.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en MyCareLink Patient Monitor de Medtronic

Fecha de publicación: 29/06/2018

Importancia: Media

Recursos afectados:

- 24950 MyCareLink Monitor, todas las versiones
- 24952 MyCareLink Monitor, todas las versiones

Descripción:

Peter Morgan de Clever Security ha reportado varias vulnerabilidades que afectan a productos MyCareLink Patient Monitor de Medtronic. Un potencial atacante con acceso físico podría conseguir acceso privilegiado al sistema operativo del monitor y leer y escribir valores de memoria arbitrarios.

Solución:

Medtronic lanzarÃi varias actualizaciones de producto que mitigarÃin las vulnerabilidades descritas en este aviso. Estas actualizaciones se aplicarÃin a los dispositivos automÃiticamente como parte de los procesos de actualización estÃindar recurrentes. AdemÃis, Medtronic ha aumentado la monitorización de seguridad de los dispositivos afectados y la infraestructura relacionada.

Medtronic recomienda a los usuarios tomar medidas defensivas adicionales para minimizar el riesgo de explotación de estas vulnerabilidades. Específicamente, los usuarios deberían:

- Mantener buenos controles físicos sobre el monitor del hogar, como la mejor mitigación para estas vulnerabilidades.
- Solo usar monitores domésticos obtenidos directamente de su proveedor de atención médica o de un representante de Medtronic para garantizar la integridad del sistema.
- Informar a su proveedor de atención médica o a un representante de Medtronic sobre cualquier comportamiento relacionado con su monitor doméstico.

Puede encontrarse mÃis información publicada por Medtronic en el siguiente enlace: https://www.medtronic.com/security

Detalle:

- Los productos afectados contienen contraseñas embebidas del sistema operativo. Un potencial atacante con acceso físico podría quitar la carcasa del dispositivo, conectarse al puerto de debug y usar la contraseña para obtener acceso privilegiado al sistema operativo. Se ha asignado el identificador CVE-2018-8870 para esta vulnerabilidad.
- Los productos afectados contienen código de depuración destinado a probar la funcionalidad de las interfaces de comunicación del monitor, incluida la interfaz entre el monitor y el dispositivo cardíaco implantable. Un potencial atacante podría aprovechar esta vulnerabilidad para leer y escribir valores de memoria arbitrarios en dispositivos cardíacos implantables a través de protocolos inalÃimbricos inductivos o de corto alcance. Se ha asignado el identificador CVE-2018-8868 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad