Boletín de abril de 2019

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en WebAccess de Advantech

Fecha de publicación: 03/04/2019

Importancia: Crítica

Recursos afectados:

- WebAccess/SCADA versiones 8.3.5 y anteriores.

Descripción:

Los investigadores Mat Powell y Natnael Samson trabajando con Trend Micro Zero Day Initiative, han reportado varias vulnerabilidades de tipo inyección de comandos, desbordamiento de búfer y control de acceso incorrecto que afectan al software WebAccess de Advantech.

Solución:

- Actualizar WebAccess a la versión 8.4.0

Detalle:

Un atacante remoto podría:

- Inyectar comandos debido a un fallo en la validación de los datos proporcionados por el usuario. Se ha reservado el identificador CVE-2019-6552 para esta vulnerabilidad.
- Ejecutar código arbitrario debido a un desbordamiento de búfer basado en pila, por un fallo en la validación de la longitud de los datos proporcionada por el usuario. Se ha reservado el identificador CVE-2019-6550 para esta vulnerabilidad.
- Causar una condición de denegación de servicio debido a una vulnerabilidad de control de acceso incorrecto. Se ha reservado el identificador CVE-2019-6554 para esta vulnerabilidad.

Etiquetas: Actualización, SCADA, Vulnerabilidad

Múltiples vulnerabilidades en productos de Bosch

Fecha de publicación: 04/04/2019

Importancia: Crítica

Recursos afectados:

- Access Easy Controller (AEC), versiones anteriores a 2.1.8.5 (inclusive), 2.1.9.0, 2.1.9.1 y 2.1.9.3
- Access Professional Edition (APE), versiones anteriores a la 3.0 y de la 3.0 a la 3.7 (solo si el componente VSDK está instalado)
- Bosch DIVAR IP 2000 y 5000
- Bosch DIVAR IP 3000
- Bosch DIVAR IP 7000, Gen1 y Gen2
- Bosch Video Client (BVC)
- Bosch Video Management Systems (BVMS), versiones 6.0, 6.5, 7.0, 7.5, 8.0 y 9.0
- Bosch Video Streaming Gateway (VSG)
- Building Integration System (BIS), versiones de la 2.2 a la 4.4 incluyendo 4.5, 4.6 y 4.6.1
- Configuration Manager
- Video Recording Manager (VRM)
- Video SDK (VSDK)

Descripción:

Se han descubierto cuatro vulnerabilidades, algunas de ellas reportadas por el investigador independiente Adrián Quirós Godoy que afectan a productos Bosch. Estas vulnerabilidades, dos de ellas críticas, son de tipo desbordamiento de búfer, control de acceso inadecuado, redireccionamiento abierto y salto de directorio. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autorizado, la lectura y escritura en el sistema mediante inyección de comandos RCP , tener acceso a directorios y archivos y ejecutar código arbitrario en el sistema.

Solución:

- La medida recomendada por el fabricante para los avisos críticos es la actualización del software de los productos afectados a una versión parcheada, según el anexo del aviso de control de acceso impropio de BT. y el anexo del aviso de desbordamiento de búfer de BT. Los parches y su procedimiento de instalación se encuentran en el área de descargas de Bosch.
- En el caso en el que no se haya lanzado aún una actualización que solucione el problema o que no sea posible realizarla, se sugiere mitigar el problema añadiendo reglas al *firewall*.

Detalle:

- Desbordamiento de búfer en el analizador (*parser*) de RCP : un atacante podría ejecutar código de manera remota al no verificarse el tamaño de entrada. Se ha reservado el CVE-2019-6957 para esta vulnerabilidad.
- Control de acceso inadecuado: el puerto RCP permite acceso sin autenticación. Un atacante remoto podría borrar o leer datos de un video. Se ha reservado el CVE-2019-6958 para esta vulnerabilidad.
- Redireccionamiento abierto: un atacante remoto podría redirigir a los usuarios a una URL con contenido malicioso. Se ha reservado el CVE-2019-8951 para esta vulnerabilidad.
- Salto de directorio: un atacante podría acceder a sistemas de archivos y acceder a archivos o directorios restringidos. Se ha reservado el CVE-2019-8952 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de corrupción de memoria en CX-Programmer de Omron

Fecha de publicación: 05/04/2019

Importancia: Media

Recursos afectados:

- CX-Programmer, versión 9.70 y anteriores.
- Common Components, versión de enero de 2019 y anteriores.

Descripción:

El investigador Esteban Ruiz de Source Incite, trabajando con Zero Day Initiative de Trend Micro, ha identificado una vulnerabilidad de uso de recursos después de la liberación de memoria en productos CX-Programmer de Omron.

Solución:

- CX-Programmer, versión 9.71
- Common Components, versión de abril de 2019

Detalle:

- Un potencial atacante podría utilizar un archivo de proyecto especialmente manipulado para explotar y ejecutar código bajo los privilegios de la aplicación, aprovechando referencias a memoria liberada. Se ha reservado el identificador CVE-2019-6556 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Rockwell Automation

Fecha de publicación: 05/04/2019

Importancia: Alta

Recursos afectados:

- Allen-Bradley Stratix 5400, 5100 y 5700, versiones anteriores a 15.2(6)E2a
- Allen-Bradley ArmorStratix 5700, versiones anteriores a 15.2(6)E2a
- Allen-Bradley Stratix 8000, versiones anteriores a 15.2(6)E0a
- Allen-Bradley Stratix 8300, versiones anteriores a 15.2(4)EA7
- Modelos Allen-Bradley Stratix 5950:
  - 1783-SAD4T0SBK9
  - 1783-SAD4T0SPK9
  - 1783-SAD2T2SBK9
  - 1783-SAD2T2SPK9

Descripción:

Rockwell Automation ha reportado múltiples vulnerabilidades de tipo consumo no controlado de recursos, errores en la gestión de recursos y validación inadecuada de datos de entrada. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autorizado provocar una situación de denegación de servicio en el dispositivo o en el servicio PTP (*Precision Time Protocol*).

Solución:

El fabricante recomienda actualizar el software de los productos afectados a las siguientes versiones (o posteriores):

- FRN 15.2(6)E2a:
  - Allen-Bradley Stratix 5400
  - Allen-Bradley Stratix 5410
  - Allen-Bradley Stratix 5700
  - Allen-Bradley ArmorStratix 5700
  - Allen-Bradley Stratix 8000
- FRN 15.2(4)EA7:
  - Allen-Bradley Stratix 8300
- Para el caso de los productos Allen-Bradley Stratix 5950 afectados, puesto que tienen el servicio IPsec deshabilitado por defecto, el fabricante recomienda no utilizar conexiones VPN IPsec. También recomienda el uso de reglas de *firewall*, ACLs y medidas relacionadas con la exposición de los dispositivos afectados.

Detalle:

- Un atacante remoto no autenticado podría enviar datos inválidos al agente de Cisco Network Plug and Play, causando una pérdida de memoria y, a su vez, un reinicio en el dispositivo afectado, provocando una condición de denegación de servicio (DoS). Se ha asignado el CVE-2018-15377 para esta vulnerabilidad.
- Un atacante no autenticado podría enviar un paquete OSPFv3 especialmente diseñado para causar un reinicio en un dispositivo afectado, provocando una condición de denegación de servicio en el mismo. Se ha asignado el CVE-2018-0466 para esta vulnerabilidad.
- Un atacante remoto no autenticado podría enviar un paquete HTTP malformado en el *framework* web de Cisco XE, causando de esta forma un desbordamiento de búfer y, por lo tanto, una condición de denegación de servicio en el dispositivo. Se ha asignado el CVE-2018-0470 para esta vulnerabilidad.
- Un atacante remoto no autenticado podría enviar paquetes IPsec malformados a un dispositivo afectado, causando su reinicio y, por lo tanto, una condición de denegación de servicio. Se ha asignado el CVE-2018-0472 para esta vulnerabilidad.
- Un atacante remoto no autenticado podría enviar un paquete PTP personalizado a un dispositivo afectado, causando de esta manera una denegación de servicio en PTP, originando una desincronización de tiempo en la red. Se ha asignado el CVE-2018-0473 para esta vulnerabilidad.
- Un atacante no autenticado podría enviar una alta tasa de paquetes de Cisco Recovery Protocol a un dispositivo afectado, llenando así la memoria de éste y produciendo una denegación de servicio. Se ha asignado el CVE-2018-15373 para esta vulnerabilidad.
- Un atacante remoto no autenticado podría enviar paquetes IPv6 maliciosos hacia un dispositivo afectado, causando su reinicio y, por lo tanto, una condición de denegación de servicio. Se ha asignado el CVE-2018-0467 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en dispositivos médicos SmartLinx Neuron 2

Fecha de publicación: 09/04/2019

Importancia: Alta

Recursos afectados:

- SmartLinx Neuron 2 versión 6.9.1

Descripción:

El investigador Patrick DeSantis, de Talos Intelligence, ha descubierto una vulnerabilidad de tipo escape de entorno restringido en el producto SmartLinx Neuron 2 de Capsule Technologies, un ordenador clínico móvil que permite la recogida automática de datos de los signos vitales. Esto podría permitir a un atacante conseguir el control total de un dispositivo de confianza en la red interna de un hospital.

Solución:

- Actualizar a la versión 10.1.

Detalle:

- Este dispositivo consta de un entorno restringido, denominado *modo kiosco*, que previene que los usuarios puedan salir de las aplicaciones en ejecución y accedan al sistema operativo subyacente. Es posible conectar un teclado USB u otros dispositivos de tipo HID para, mediante una serie de pulsaciones de teclado, salir de este entorno restringido y acceder al sistema operativo Microsoft Windows con permisos de administrador. Este acceso podría proporcionar a un atacante el control total de un dispositivo de confianza en la red interna de un hospital. Se ha reservado el identificador CVE-2019-5024 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en productos Siemens

Fecha de publicación: 09/04/2019

Importancia: Crítica

Recursos afectados:

- RUGGEDCOM ROX II, todas las versiones anteriores a la V2.13.0
- SINEMA Remote Connect Client, todas las versiones anteriores a la V2.0 HF1
- SINEMA Remote Connect Server, todas las versiones anteriores a la V2.0
- Spectrum Power^{TM} 4: versión con Web Office Portal
- SIMATIC CP443-1 OPC UA, todas las versiones
- SIMATIC ET 200 Open Controller CPU 1515SPPC2, todas las versiones
- SIMATIC IPC DiagMonitor, todas las versiones
- SIMATIC NET PC Software, todas las versiones
- SIMATIC RF188C, todas las versiones
- SIMATIC RF600R, todas las versiones
- SIMATIC S7-1500 CPU family, todas las versiones anteriores a la V2.5

- SIMATIC S7-1500 Software Controller, todas las versiones anteriores a la V2.5
- SIMATIC WinCC OA, todas las versiones anteriores a la V3.15-P018
- SIMATIC WinCC Runtime Advanced, Comfort, HSP Comfort y Mobile, todas las versiones
- SINEC-NMS, todas las versiones
- SINEMA Server, todas las versiones
- SINUMERIK OPC UA Server, todas las versiones anteriores a la V2.1
- TeleControl Server Basic, todas las versiones
- CP1604, todas las versiones
- CP1616, todas las versiones
- SIMATIC RF185C, todas las versiones
- SIMATIC CP443-1 y CP343-1 Advanced, todas las versiones
- SIMATIC CP443-1 OPC UA y CP443-1 Advanced, todas las versiones
- SIMATIC ET 200 SP Open Controller CPU1515SP PC, todas las versiones anteriores a la V2.1.6
- SIMATIC ET 200 SP Open Controller CPU1515SP PC2, todas las versiones
- SIMATIC HMI Comfort Outdoor Panels 7" & 15", todas las versiones
- SIMATIC HMI Comfort Panels 4" - 22", todas las versiones
- SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 y KTP900F, todas las versiones
- SIMATIC IPC DiagMonitor, todas las versiones
- SIMATIC RF181-EIP, RF182C, RF186C, RF188C y RF600R, todas las versiones
- SIMATIC S7-1500 CPU family, todas las versiones
- SIMATIC S7-1500 Software Controller, todas las versiones
- SIMATIC S7-300 CPU family, todas las versiones anteriores a la V3.X.16
- SIMATIC S7-400 PN (incl. F) V6 y posteriores, todas las versiones
- SIMATIC S7-400 PN/DP V7 (incl. F), todas las versiones
- SIMATIC S7-PLCSIM Advanced, todas las versiones
- SIMATIC Teleservice Adapter IE Advanced, Basic y Standard, todas las versiones
- SIMATIC WinAC RTX 2010, todas las versiones
- SIMATIC WinCC Runtime Advanced, todas las versiones
- SIMOCODE pro V EIP, todas las versiones
- SIMOCODE pro V PN, todas las versiones
- SINAMICS G130 V4.6, todas las versiones
- SINAMICS G130 V4.7 y SP1, todas las versiones
- SINAMICS G130 V4.8, todas las versiones anteriores a la 4.8 HF6
- SINAMICS G130 V5.1, todas las versiones
- SINAMICS G130 V5.1 SP1, todas las versiones anteriores a la V5.1 SP1 HF4
- SINAMICS G150 V4.6, V4.7 y V4.7 SP1, todas las versiones
- SINAMICS G150 V4.8, todas las versiones anteriores a la V4.8 HF6
- SINAMICS G150 V5.1, todas las versiones
- SINAMICS G150 V5.1 SP1, todas las versiones anteriores a la V5.1 SP1 HF4
- SINAMICS S120 V4.6, V4.7 y V4.7 SP1, todas las versiones
- SINAMICS S120 V4.8, todas las versiones anteriores V4.8 HF6
- SINAMICS S120 V5.1, todas las versiones
- SINAMICS S120 V5.1 SP1, todas las versiones anteriores a la V5.1 SP1 HF4
- SINAMICS S150 V4.6, V4.7 y V4.7 SP1, todas las versiones
- SINAMICS S150 V4.8, todas las versiones anteriores V4.8 HF6
- SINAMICS S150 V5.1, todas las versiones
- SINAMICS S150 V5.1 SP1, todas las versiones anteriores a la V5.1 SP1 HF4
- SINAMICS S210 V5.1 y V5.1 SP1, todas las versiones
- SITOP Manager, PSU8600, UPS1600, todas las versiones
- TIM 1531 IRC, todas las versiones

Descripción:

La empresa Applied Risk ha gestionado la vulnerabilidad con identificador CVE-2019-6579 en colaboración con el equipo de Siemens ProductCERT. Las vulnerabilidades restantes han sido gestionadas por el propio fabricante. Las diferentes vulnerabilidades detectadas son de tipo manipulación del demonio Quagga BGP, desbordamientos de búfer, acceso no autorizado y envío de paquetes especialmente diseñados. Permitirían a un atacante ejecutar código remotamente, originar denegaciones de servicio y realizar modificaciones de configuración en los dispositivos afectados.

Solución:

- Para los dispositivos RUGGEDCOM ROX II, se recomienda actualizar a la versión V2.13.0. Como medidas de mitigación, Siemens recomienda a sus clientes aplicar las siguientes acciones:
  - Deshabilitar el servicio de rutas BGP si no se está utilizando.
  - Configurar las contraseñas BGP para autenticar vecinos BGP.
- Para los dispositivos SINEMA Remote Connect Client, se recomienda actualizar a la versión V2.0 HF1.
- En el caso de los dispositivos SINEMA Remote Connect Server, se recomienda actualizar a la versión V2.0. Como medidas de mitigación, Siemens recomienda a sus clientes aplicar las siguientes acciones:
  - Deshabilitar la autenticación NTLM para mitigar las vulnerabilidades CVE-2018-16890 y CVE-2019-3822.
  - Deshabilitar el servicio SMTP para mitigar la vulnerabilidad CVE-2019-3823.
  - Aplicar las estrategias de mitigación apropiadas.
- Para los sistemas Spectrum Power™ 4, se recomienda eliminar el *bugfix* bf-47456_PE_WOP_fix. Además, Siemens recomienda deshabilitar el servidor web o limitar el acceso al mismo mediante un cortafuegos externo.
- Para el resto de dispositivos afectados por las vulnerabilidades con identificadores CVE-2019-6575 y CVE-2019-6568, visitar los apartados *WORKAROUNDS AND MITIGATIONS* de los avisos de Siemens correspondientes enlazados en la sección de *Referencias*.

Detalle:

- Un potencial atacante local no autenticado con acceso al servidor mediante los puertos 80/TCP y 443/TCP podría realizar una inyección de comandos para, de esta manera, ejecutarlos con privilegios administrativos. Se ha reservado el identificador CVE-2019-6579 para esta vulnerabilidad.
- Un potencial atacante podría suplantar mensajes de BGP UPDATE y aprovechar una liberación doble de la memoria para provocar una denegación de servicio o ejecutar código arbitrario. Se ha asignado el identificador CVE-2018-5379 para esta vulnerabilidad.
- El resto de vulnerabilidades tienen asignados los siguientes identificadores: CVE-2018-5380, CVE-2018-5381, CVE-2019-6568, CVE-2018-14618, CVE-2018-16890 y CVE-2019-3822. En cuanto a los reservados, son los siguientes: CVE-2019-6575 y CVE-2019-6570.

Etiquetas: Siemens, Vulnerabilidad

Vulnerabilidad en Modbus Serial Driver de

Schneider

Fecha de publicación: 10/04/2019

Importancia: Alta

Recursos afectados:

Modbus Serial Driver en las siguientes versiones:

- Para SO Windows 64-bits V3.17 IE 37 y anteriores.
- Para SO Windows 32-bits V2.17 IE 27 y anteriores.
- Driver Suite versión V14.12 y anteriores.

Descripción:

El investigador Reid Wightman de Dragos ha identificado una vulnerabilidad de tipo referencias a recurso controlado externamente en productos Modbus Serial Driver que podría permitir a un atacante conseguir acceso dentro del sistema.

Solución:

- Aplicar el siguiente parche

Detalle:

- Un atacante, aprovechando referencias a un recurso controlado externamente, podría conseguir acceso a los archivos del sistema con permiso de escritura solo disponibles para usuarios con privilegios. Se ha reservado el CVE-2018-7824 para esta vulnerabilidad.

Etiquetas: Schneider Electric, Vulnerabilidad

Acceso a rutas no controlado en componentes SPRECON de Sprecher Automation

Fecha de publicación: 10/04/2019

Importancia: Baja

Recursos afectados:

- *Firmware* de SPRECON-E-C/P versiones entre la 8.52 y la 8.62, en las variantes de hardware PU244x.

Descripción:

Sprecher Automation ha publicado una vulnerabilidad de tipo *path traversal*. Un atacante con acceso a la red donde se encuentran los dispositivos afectados y que, a su vez, esté autenticado en la aplicación web, podría descargar y consultar archivos que contienen información sensible.

Solución:

- Se aconseja actualizar a las últimas versiones de *firmware* disponibles (8.52g y 8.56f) que solventan las vulnerabilidades.
- Si el acceso controlado por roles (*RBAC*) está activado, no es posible explotar esta vulnerabilidad sin tener credenciales de usuario válidas. El fabricante aconseja tener siempre activada la autenticación de usuarios en todas las interfaces. En cualquier caso, se aconseja segmentar la red para proteger las interfaces de los respectivos interfaces.

Detalle:

- Esta vulnerabilidad es del tipo *Path Traversal*. Un atacante con acceso web al dispositivo afectado por la vulnerabilidad podría acceder a ficheros con los permisos del servidor web (www-data).

Etiquetas: Actualización, Vulnerabilidad

Acceso a servicio no documentado en dispositivos de WAGO

Fecha de publicación: 12/04/2019

Importancia: Crítica

Recursos afectados:

- Series 750-88x con firmware anterior a la versión 14:
  - 750-330
  - 750-352/
  - 750-829
  - 750-831
  - 750-852
  - 750-880/
  - 750-881
  - 750-882
  - 750-884/
  - 750-885
  - 750-889

- Series 750-87x
  - 750-830 con firmware anterior a la versión FW06.
  - 750-849 con firmware anterior a la versión FW08.
  - 750-871 con firmware anterior a la versión FW11.
  - 750-872 con firmware anterior a la versión FW07.
  - 750-873 con firmware anterior a la versión FW07.

Descripción:

El investigador de seguridad Jörn Schneeweisz del CERT-Bund ha coordinado esta vulnerabilidad junto con el propio CERT-Bund. Esta vulnerabilidad de tipo uso de contraseñas embebidas, podría permitir a un atacante remoto cambiar las configuraciones del dispositivo o de la aplicación del mismo.

Solución:

- Se aconseja actualizar el dispositivo a la última versión de firmware disponible en función del dispositivo afectado y de la versión de firmware vulnerable.
- En caso de no poder actualizar la versión de firmware, se aconseja seguir las siguientes pautas:
  - Restringir el acceso a la red donde se encuentra el dispositivo afectado con el servidor web activo.
  - Restringir el acceso al propio dispositivo.
  - No proporcionar accesos directos desde Internet al dispositivo.

Detalle:

- El uso de contraseñas embebidas podría permitir a un atacante cambiar la configuración del dispositivo y acceder con privilegios a la administración de la web para bloquear a otros usuarios del dispositivo, abrir puertos de red previamente cerrados, utilizar el servicio FTP, intercambiar la aplicación o eliminarla. Se ha reservado el identificador CVE-2019-10712 para esta vulnerabilidad.

Etiquetas: Navegador, Vulnerabilidad

Desbordamientos de búfer en CNCSoft de Delta Industrial Automation

Fecha de publicación: 17/04/2019

Importancia: Alta

Recursos afectados:

- CNCSoft ScreenEditor versión 1.00.88 y anteriores.

Descripción:

El investigador de seguridad Natnael Samson y un investigador anónimo, en colaboración con Zero Day Initiative (ZDI) de Trend Micro, han reportado estas vulnerabilidades de tipo desbordamiento de búfer que podrían permitir a un atacante revelar información, ejecutar código remoto o provocar un funcionamiento incorrecto de la aplicación.

Solución:

- Actualizar a la versión 1.00.89

Detalle:

- La incorrecta validación de los parámetros de entrada antes de copiar los datos de los archivos de proyecto en la pila o en la memoria dinámica (heap), permite el desbordamiento de búfer. Un atacante podría procesar ficheros de proyecto especialmente diseñados para ejecutar código remoto. Se han reservado los identificadores CVE-2019-10947 y CVE-2019-10951 para estas vulnerabilidades.
- La incorrecta validación de los parámetros de entrada antes de copiar los datos de los archivos de proyecto podría permitir a un atacante la lectura fuera de límite, consiguiendo la divulgación de información. Se ha reservado el identificador CVE-2019-10949 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de manipulación del tiempo de ciclo en PLC en varios fabricantes

Fecha de publicación: 17/04/2019

Importancia: Alta

Recursos afectados:

- ABB 1SAP120600R0071 PM554-TP-ETH
- Phoenix Contact 2700974 ILC 151 ETH
- Schneider Modicon M221
- Siemens
  - 6ES7211-1AE40-0XB0 Simatic S7-1211
  - 6ES7314-6EH04-0AB0 Simatic S7-314
  - 6ED1052-1CC01-0BA8 Logo! 8
- WAGO
  - Controlador 750-889 KNX IP
  - Controlador 750-8100 PFC100
  - Controlador 750-880 ETH
  - Controlador 750-831 BACnet/IP

Descripción:

Los investigadores de seguridad Matthias Niedermaier (Hochschule Augsburg), Jan-Ole Malchow (Freie Universita¨t Berlin) y Florian Fischer (Hochschule Augsburg) han reportado una vulnerabilidad de consumo no controlado de recursos, que permitiría a un atacante realizar una denegación de servicio en el dispositivo afectado.

Solución:

Cada fabricante ha proporcionado distintas soluciones para la vulnerabilidad:

- ABB: no clasifica esta vulnerabilidad como tal, sino que asocia el problema a una mala configuración del controlador del PLC que se configuró de manera predeterminada en la fábrica. Esta configuración errónea puede solventarse estableciendo una apropiada combinación de la prioridad de la tarea, el tiempo de ciclo de la misma y la configuración de vigilancia (*watchdog*). El fabricante aconseja consultar el capítulo *Onboard Ethernet Handling in CPU Firmware* para más información.
- Phoenix Contact: clasifica la vulnerabilidad como un problema conocido, no solucionado para productos antiguos. Los productos que poseen actualmente en el mercado, proporcionan contramedidas para mitigar el impacto en las funcionalidades relacionadas con la seguridad. Para más información, puede consultarse la nota publicada por la compañía.
- Schneider Electric: las correcciones para solventar esta vulnerabilidad se encuentran en la versión de firmware v1.10.0.0 del Modicon M221 y la v1.0 para el software EcoStruxure Machine Expert - Basic. Otra opción es ejecutar la herramienta de actualización de software de Schneider Electric para descargar e instalar la versión 1.0 de EcoStruxure Machine Expert - Basic. La compañía ha publicado un aviso de seguridad (SEVD-2019-045-01).
- Siemens: ha investigado y valorado los resultados expuestos en el informe de la vulnerabilidad que se le ha presentado y concluye que en dicho informe no se demuestra una vulnerabilidad válida para sus PLC.
- WAGO: recomienda a sus clientes que utilicen los dispositivos afectados bajo redes cerradas o que protejan sus comunicaciones con un cortafuegos para evitar accesos no autorizados. Otra mitigación recomendada es limitar el tráfico de red a través de la función de límite de velocidad de conmutación de acuerdo con las necesidades de la aplicación.

Detalle:

- Los dispositivos afectados son susceptibles a ataques de denegación de servicio originados mediante la inundación de paquetes en la red donde se encuentran. Una alta carga de paquetes en la red, puede consumir energía de la CPU del dispositivo afectado, de tal manera que el tiempo de ciclo configurado puede ser manipulado y, consecuentemente, su funcionamiento puede verse afectado. Se ha reservado el identificador CVE-2019-10953 para esta vulnerabilidad.

Etiquetas: Actualización, Schneider Electric, Siemens, Vulnerabilidad

---

Múltiples vulnerabilidades en productos CODESYS

Fecha de publicación: 22/04/2019

Importancia: Crítica

Recursos afectados:

Todas las variantes de los siguientes productos CODESYS V3 que utilicen versiones anteriores a la V3.5.14.20 y contengan el componente CmpGateway están afectadas por las vulnerabilidades, independientemente del tipo de CPU o Sistema operativo.

- CODESYS Control para BeagleBone
- CODESYS Control para emPC-A/iMX6
- CODESYS Control para IOT2000
- CODESYS Control para Linux
- CODESYS Control para PFC100
- CODESYS Control para PFC200
- CODESYS Control para Raspberry Pi
- CODESYS Control V3 Runtime System Toolkit
- CODESYS Gateway V3
- CODESYS V3 Development System

Descripción:

El investigador de seguridad Martin Hartmann, de Cirosec GmbH, ha reportado dos vulnerabilidades. Una de ellas es crítica del tipo valores aleatorios no controlados y asignación de propiedad no verificada, y la otra de criticidad alta del tipo asignación de memoria. Ambas pueden ser explotadas remotamente. La explotación exitosa de estas vulnerabilidades por parte de un atacante podría originar denegaciones de servicio y cortes en las comunicaciones.

Solución:

El fabricante ha publicado una nueva versión de software (V3.5.14.20) que mitiga estas vulnerabilidades.

Detalle:

- Vulnerabilidad crítica de asignación de valores aleatorios no controlada: CODESYS Gateway no usa valores aleatorios adecuados para identificar el canal de comunicación y verifica de manera insuficiente la propiedad del canal. La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto cierre los canales de comunicación existentes. Si el canal no estaba protegido por una comunicación cifrada, un atacante remoto también podría enviar paquetes especialmente diseñados a un PLC dentro de una sesión de usuario ya establecida. Se ha reservado el identificador CVE-2019-9010 para esta vulnerabilidad.
- Vulnerabilidad de criticidad alta de asignación de memoria no controlada: un atacante remoto podría enviar peticiones especialmente diseñadas y realizar así asignaciones de memoria no controladas en los productos CODESYS afectados. La explotación exitosa de esta vulnerabilidad originaría denegaciones de servicio. Se ha reservado el identificador CVE-2019-9012 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en FCR Capsula X/Carbon X de Fujifilm

Fecha de publicación: 24/04/2019

Importancia: Crítica

Recursos afectados:

- CR-IR 357 FCR Carbon X
- CR-IR 357 FCR XC-2
- CR-IR 357 FCR Capsula X

Descripción:

Los investigadores Marc Ruef y Rocco Gagliardi de Scip AG, han reportado varias vulnerabilidades de tipo consumo de recursos sin control y control de accesos inadecuado que afecta a los dispositivos FCR Capsula X/Carbon X de Fujifilm. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto causar una condición de denegación de servicio u obtener acceso sin autorización al dispositivo pudiendo llegar a ejecutar código arbitrario.

Solución:

- Fujifilm recomienda configurar el sistema con la funcionalidad "Secure Host". Con esta configuración el dispositivo ignora todo el tráfico de red que no sea de la dirección IP de la consola de adquisición de imágenes de Fujifilm. Sin embargo, esta configuración impide que más de una consola de adquisición de imágenes comparta la unidad lectora CR-IR 357. Si la unidad lectora no está compartida, los usuarios deben ponerse en contacto con Fujifilm para solicitar que se habilite la funcionalidad "Secure Host". Si la unidad lectora es compartida, los usuarios deben ponerse en contacto con Fujifilm para discutir las opciones disponibles.
- Adicionalmente Fujifilm recomienda aplicar controles compensatorios de seguridad en la red del usuario. Se deben tomar medidas para garantizar que solo los dispositivos y personal autorizados tengan acceso a la red. Las redes públicas o invitadas deben estar segmentadas, o los usuarios deben usar VLAN para segregar el tráfico público de la red privada. Fujifilm también recomienda implementar controles administrativos y técnicos.

Detalle:

- Cuando el dispositivo sufre un desbordamiento de paquetes TCP requiere un reinicio manual, lo que provoca una condición de denegación de servicio. Se ha asignado el identificador CVE-2019-10948 para esta vulnerabilidad.
- El dispositivo proporciona servicios telnet inseguros los cuales carecen de requisitos de autenticación. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto el acceso al sistema operativo subyacente. Se ha asignado el identificador CVE-2019-10950 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en AXC F 2152 de Phoenix Contact

Fecha de publicación: 24/04/2019

Importancia: Alta

Recursos afectados:

- AXC F 2152 y Starterkit AXC F 2152, versión de firmware 1.x

Descripción:

El investigador Zahra Khani, de Firmalyzer SPRL, y OPC Foundation han publicado múltiples vulnerabilidades que afectan a los dispositivos AXC F 2152 de Phoenix Contact. La explotación exitosa de estas vulnerabilidades podría afectar a la confidencialidad, la integridad o la disponibilidad del dispositivo.

Solución:

- Phoenix Contact recomienda actualizar los dispositivos a la versión de Firmware y de PLCnext Engineer 2019.0 LTS o posterior para solucionar estas vulnerabilidades.
- Adicionalmente, para la vulnerabilidad cuyo identificador es CVE-2018-7559, Phoenix Contact recomienda deshabilitar la política de seguridad Basic128Rsa15 en la configuración de los servidores OPC y utilizar siempre Basic256 o superior.

Detalle:

- La versión de firmware 1.x del dispositivo AXC F 2152 hace uso de versiones antiguas de software de terceros que son vulnerables. El listado de identificadores de dichas vulnerabilidades es el siguiente: CVE-2016-6301, CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-15906, CVE-2016-1247, CVE-2018-1000117, CVE-2017-9233, CVE-2017-3735, CVE-2017-3731, CVE-2017-3738, CVE-2017-3737, CVE-2018-0737, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, CVE-2018-1000122, CVE-2018-1000301, CVE-2017-8817, CVE-2018-1000120, CVE-2018-1000121, CVE-2016-9952, CVE-2016-9953, CVE-2017-1000101, CVE-2017-8816, CVE-2017-1000254, CVE-2017-1000100, CVE-2017-1000257, CVE-2018-1000005, CVE-2016-7141, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-7444, CVE-2017-9023, CVE-2018-5388, CVE-2017-9022, CVE-2017-11185, CVE-2015-9251, CVE-2016-7103.
- Un atacante remoto podría realizar un *man in the middle* y causar una denegación de servicio en el protocolo de *fuzzing* de PC WORX Engineer, deteniendo el servicio del PLC. Para restablecer el servicio se debe reiniciar el dispositivo o restablecerlo manualmente mediante la consola Linux. Se ha reservado el identificador CVE-2019-10997 para esta vulnerabilidad.
- Un atacante con acceso físico al dispositivo podría extraer la tarjeta SD y manipular sus datos, lo que permitiría evitar la autenticación del dispositivo. Se ha reservado el identificador CVE-2019-10998 para esta vulnerabilidad.
- Un atacante remoto podría aprovechar una vulnerabilidad en la política de seguridad Basic128Rsa15 del servidor OPC enviando *tokens* de identificación de usuario especialmente diseñados. Esto permitiría al atacante descifrar contraseñas de políticas más robustas como Basic256Sha256. Se ha asignado el identificador CVE-2018-7559 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Redirector malicioso en productos Rockwell

Automation

Fecha de publicación: 24/04/2019

Importancia: Alta

Recursos afectados:

- MicroLogix 1400 controllers:
  - Serie A todas las versiones
  - Serie B versión 15.002 y anteriores
- MicroLogix 1100 controllers versión 14.00 y anteriores
- CompactLogix 5370 L1 y L2 controllers versión 30.014 y anteriores
- CompactLogix 5370 L3 con CompactLogix GuardLogix controllers versión 30.014 y anteriores

Descripción:

Los investigadores Josiah Bryan y Geancarlo Palavicini han reportado esta vulnerabilidad del tipo redirector malicioso que afecta a varios productos de Rockwell Automation. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado redirigir al usuario a una website maliciosa.

Solución:

Rockwell Automation proporciona las siguientes soluciones para los equipos afectados:

- MicroLogix 1400 controllers serie A deshabilitar el parámetro HTTP en el dispositivo.
- MicroLogix 1400 controllers serie B aplicar FRN 15.003 o posterior.
- MicroLogix 1100 controllers aplicar FRN 15.000 o posterior.
- CompactLogix 5370 L1 controllers, L2 controllers y L3 controllers aplicar versión 31.011 o posterior

Detalle:

Un atacante remoto no autenticado podría introducir un enlace malicioso para redirigir a los usuarios a una website maliciosa, donde el atacante podría descargar o ejecutar malware en la máquina del usuario. Se ha reservado el identificador CVE-2019-10955 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad