Boletín de marzo de 2019

Avisos de Sistemas de Control Industrial

Desbordamiento de búfer en WebAccess de Advantech

Fecha de publicación: 01/03/2019

Importancia: Crítica

Recursos afectados:

- WebAccess

Descripción:

Existe una vulnerabilidad de severidad crítica que afecta a los dispositivos WebAccess de Advantech. Esta podría permitir a un atacante remoto sin autenticación la ejecución de código de manera arbitraria.

Solución:

- Restringir la interacción con el servicio a máquinas de confianza.

Detalle:

- La vulnerabilidad se encuentra presente en los ejecutables *spchapi.exe* y *tv_enua.exe* a través de la llamada *IOCTL 0x2711* en el proceso *webvrpcs*. Debido a una falta de validación de la longitud de los datos proporcionados por el usuario antes de que sean copiados a un búfer basado en pila de longitud fija. Un atacante remoto podría aprovechar esta vulnerabilidad para la ejecución de código con permisos de administrador.

Etiquetas: 0day, Vulnerabilidad

Cross-site scripting en dispositivos de PSI GridConnect GmbH

Fecha de publicación: 01/03/2019

Importancia: Alta

Recursos afectados:

- Telecontrol Gateway 3G versiones 4.2.21, 5.0.27, 6.0.16 y anteriores
- Telecontrol Gateway XS-MU versiones 4.2.21, 5.0.27, 5.1.19, 6.0.16 y anteriores
- Telecontrol Gateway VM versiones 4.2.21, 5.0.27, 5.1.19, 6.0.16 y anteriores
- Smart Telecontrol Unit TCG versions 5.0.27, 5.1.19, 6.0.16 y anteriores
- IEC104 Security Proxy version 2.2.10 y anteriores

Descripción:

El investigador Can Kurnaz ha identificado una vulnerabilidad de tipo cross-site scripting (XSS) que afecta a varios dispositivos de PSI GridConnect GmbH y que podría permitir a un atacante ejecutar código de manera arbitraria en la aplicación objetivo.

Solución:

- PSI recomienda a los usuarios actualizar a las versiones 5.1.20, 6.0.17 e IEC104 Security Proxy versión 2.2.11.
- Las versiones 4.2.x y 5.0.x ya no tendrán soporte

Detalle:

- Una vulnerabilidad de cross-site scripting debida a una neutralización incorrecta de las entradas HTML, JavaScript o VBScript durante la generación de la página web, podría permitir a un atacante ejecutar código de manera arbitraria. Se ha asignado el identificador CVE-2019-6528 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Denegación de servicio y ejecución remota de código en RSLinx Classic de Rockwell

Fecha de publicación: 05/03/2019

Importancia: Crítica

Recursos afectados:

- RSLinx Classic versión v4.10.00 y anteriores

Descripción:

Tenable ha reportado a Rockwell Automation una vulnerabilidad del tipo desbordamiento de búfer que afecta a sus dispositivos RSLinx Classic que podría dar lugar a una condición de denegación de servicio o a la ejecución remota de código.

Solución:

- Aplicar el siguiente parche.

Detalle:

- La validación inadecuada de los datos de entrada en un fichero dll de RSLinx Classic, donde los datos de una solicitud Open Forward son pasados a un búfer de longitud fija, podría permitir a un atacante remoto detener la aplicación RSLinx.exe dando lugar a una condición de denegación de servicio o la ejecución de código. Se ha asignado el identificador CVE-2019-6553 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de salto de directorio en WirelessHART-Gateways de PEPPERL FUCHS

Fecha de publicación: 07/03/2019

Importancia: Media

Recursos afectados:

- WHA-GW-*

Descripción:

El investigador Hamit CIBO identificó una vulnerabilidad de tipo salto de directorio que afecta a los dispositivos WirelessHART Gateway. La explotación de dicha vulnerabilidad permitiría a atacantes remotos no autenticados acceder a archivos arbitrarios.

Solución:

PEPPERL FUCHS recomienda actualizar los dispositivos a la última versión de firmware que soluciona esta vulnerabilidad:

- WHA-GW-*-ETH a la versión 03.00.08
- WHA-GW-*-ETH.EIP a la versión 02.00.01

Detalle:

- Un atacante podría explotar dicha vulnerabilidad con el fin de obtener acceso a los ficheros y directorios restringidos almacenados en el dispositivo, manipulando los parámetros de los archivos que hacen referencia a los mismos. Las peticiones HTTP entrantes que utilizan *fcgi-bin/wgsetcgi* y un parámetro de nombre de archivo podrían permitir el salto de directorio. Se ha asignado el identificador CVE-2018-16059 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de escalado de privilegios en WebAccess de Advantech

Fecha de publicación: 08/03/2019

Importancia: Alta

Recursos afectados:

- WebAccess

Descripción:

Fritz Sands, de Zero Day Initiative, ha reportado una vulnerabilidad de tipo escalado de privilegios que afecta a los productos WebAccess de Advantech. La explotación exitosa de dicha vulnerabilidad podría permitir a un atacante local escalar privilegios.

Solución:

- Actualmente, no existe un parche para dicha vulnerabilidad, se recomienda restringir la interacción con el servicio a únicamente máquinas de confianza.

Detalle:

- Existe una vulnerabilidad de tipo escalado de privilegios existente dentro del control de acceso durante la instalación del producto. Dicha instalación debilita las restricciones del control de acceso existente de los archivos de sistema actuales, introduciendo a su vez restricciones débiles a los archivos nuevos. Un atacante puede utilizar dicha vulnerabilidad para escalar privilegios hasta un nivel de administrador.

Etiquetas: 0day, Windows

Aislamiento inadecuado de puerto espejo en Scalance X de Siemens

Fecha de publicación: 12/03/2019

Importancia: Media

Recursos afectados:

- Scalance X-200 y X-300, todas las versiones
- Scalance XP/XC/XF-200, todas las versiones anteriores a la 4.1

Descripción:

Siemens ha identificado una vulnerabilidad de tipo aislamiento inadecuado en el puerto espejo que afecta a los switches ScalanceX y podría permitir a un atacante introducir información en una red a través del puerto espejo si tiene la función de monitorización de barrera activada.

Solución:

- Los usuarios de los productos Scalance XP/XC/XF-200 deben actualizar a la versión 4.1.
- Para el resto de los productos afectados, Siemens recomienda aplicar principios de defensa en profundidad y, especialmente, asegurarse de que ningún dispositivo que transmita información a la red espejo es operado dentro de ella.

Detalle:

- La barrera de monitorización de los productos afectados no bloquea adecuadamente la transmisión de datos a través del puerto espejo a la red replicada. Esto podría permitir a un atacante transmitir paquetes maliciosos a sistemas en la red duplicada, influyendo en su configuración y tiempo de ejecución. Se ha reservado el identificador CVE-2019-6569 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en productos de Schneider Electric

Fecha de publicación: 13/03/2019

Importancia: Alta

Recursos afectados:

- VideoXpert OpsCenter, versiones anteriores a la 3.1
- U.motion Builder, versión 1.3.4

Descripción:

Los investigadores Julien Ahrens de RCE Security y Osama Radwan han identificado varias vulnerabilidades de tipo elemento de ruta de búsqueda no controlado e inyección SQL que afectan a varios productos de Schneider Electric. Un potencial atacante remoto podría llegar a invocar librerías DLL incorrectas o ejecutar código arbitrario.

Solución:

- Los usuarios de U.motion Builder deben eliminar inmediatamente el producto, ya que se encuentra retirado y no recibirá más soporte.
- Los usuarios de VideoXpert OpsCenter deben actualizar a la versión 3.1.

Detalle:

- Un potencial atacante local podría hacer que el sistema invoque librerías DLL incorrectas. Se ha reservado el identificador CVE-2018-7840 para esta vulnerabilidad.
- Un potencial atacante remoto, mediante una inyección SQL, podría ejecutar código no deseado haciendo uso de caracteres no adecuados en las entradas. Se ha reservado el identificador CVE-2018-7841 para esta vulnerabilidad.

Etiquetas: Schneider Electric, Vulnerabilidad

Verificación inadecuada de condiciones inusuales en Triconex TriStation Emulator de Schneider Electric

Fecha de publicación: 15/03/2019

Importancia: Alta

Recursos afectados:

- Triconex TriStation Emulator Version 1.2.0

Descripción:

El investigador independiente Tom Westenberg ha identificado una vulnerabilidad de tipo verificación inadecuada de condiciones inusuales. Un atacante remoto podría ejecutar una denegación de servicio (DoS) afectando al emulador.

Solución:

Todavía no hay una solución para esta vulnerabilidad, pero Schneider Electric nos aconseja:

- Ubicar las redes de sistemas de control y los dispositivos remotos detrás de los cortafuegos y aislarlos de las redes corporativas.
- Mejores controles físicos para que el personal no autorizado no tenga acceso al SCI.
- Escanear los dispositivos extraíbles en una red aislada antes de usarlos en un terminal de SCI.
- Cuando se requiera acceso remoto, utilizar VPN para mayor seguridad en la red.

Detalle:

- Un atacante remoto podría causar una denegación de servicio haciendo uso de un paquete especialmente diseñado que bloquearía el emulador. Se ha reservado el identificador CVE-2018-7803 para esta vulnerabilidad.

Etiquetas: Schneider Electric, Vulnerabilidad

Vulnerabilidad de elemento de ruta de búsqueda no controlado en Sentinel UltraPro de Gemalto

Fecha de publicación: 15/03/2019

Importancia: Media

Recursos afectados:

- Sentinel UltraPro Client Library *ux32w.dll*, versiones 1.3.0, 1.3.1 y 1.3.2

Descripción:

El investigador ADLab de Venustech ha reportado una vulnerabilidad de elemento de ruta de búsqueda no controlado. Un atacante podría ejecutar código o comandos arbitrarios.

Solución:

- Los usuarios afectados deben actualizar a la versión 1.3.3 que soluciona esta vulnerabilidad.

Detalle:

- Existe una vulnerabilidad de elemento de ruta de búsqueda no controlado que podría permitir a un atacante cargar y ejecutar un fichero malicioso desde la librería *ux32.dll* en Sentinel UltraPro. Se ha asignado el identificador CVE-2019-6534 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en móviles ecom de PEPPERL FUCHS

Fecha de publicación: 15/03/2019

Importancia: Alta

Recursos afectados:

- i.roc Ci70-Ex
- Cx70-Ex
- CT50-Ex
- Pad-Ex 01
- Tab-Ex 01
- Smart-Ex 01
- Smart-Ex 201
- Ex-Handy 09
- Ex-Handy 209

Descripción:

Ben Seri y Gregory Vishnepolsky de Armis han identificado varios vectores de ataque relacionados con las comunicaciones Bluetooth y han publicado la vulnerabilidad BlueBorne. Un atacante podría tomar el control del dispositivo y ejecutar código arbitrario o acceder a datos sensibles.

Solución:

PEPPERL FUCHS recomienda actualizar los dispositivos, según el que esté afectado, con el firmware correspondiente:

- CT50-Ex Android, Smart-Ex 01 y Smart-Ex 201: FOTA-Update
- CT50-Ex Windows y Pad-Ex 01: Microsoft Update

Detalle:

- Un atacante remoto no autenticado podría obtener información privada sobre el dispositivo o usuario, ejecutar código arbitrario o realizar un ataque *man-in-the-middle* (MitM). Se han asignado los identificadores CVE-2017-0781, CVE-2017-0785, CVE-2017-0782, CVE-2017-0783, CVE-2017-8628 para estas vulnerabilidades.

Etiquetas: Comunicaciones, Móviles, Vulnerabilidad

Múltiples vulnerabilidades en Field Xpert de ENDRESS HAUSER

Fecha de publicación: 20/03/2019

Importancia: Alta

Recursos afectados:

- PDA Field Xpert SFX350 y SFX370.
- Tablet PC Field Xpert SMT70 para la configuración de equipos.

Descripción:

El investigador Mathy Vanhoef de imec-DistriNet ha reportado varias vulnerabilidades que afectan a los dispositivos Field Xpert de Endress Hauser con wifi habilitado y que podrían permitir a un atacante, dentro del rango de actuación del wifi, realizar ataques de reproducción, descifrado y falsificación de paquetes.

Solución:

- Para los dispositivos Field Xpert SFX350 y SFX370, que utilizan Windows Mobile, Endress Hauser recomienda aplicar la última actualización de seguridad proporcionada por Microsoft (SR18012500_802T_Cx70_WM65_ALL.CAB).
- Para el dispositivo Field Xpert SMT70, con Windows 10 Pro 1703 64 EN, Endress Hauser recomienda actualizar a la última versión disponible de Windows.

Detalle:

- Se han identificado múltiples vulnerabilidades dentro del estándar WPA2 que podrían permitir a un atacante la reinstalación de la clave temporal PTK (Pairwise Transient Key), una clave de grupo o una de integridad en un cliente inalámbrico o punto de acceso remoto, pudiendo así descifrar o inyectar paquetes mediante ataques man-in-the-middle entre el punto de acceso y el cliente. Se han asignado los identificadores CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088 para estas vulnerabilidades.

Etiquetas: Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en protocolo de telemetría Conexus de Medtronic

Fecha de publicación: 22/03/2019

Importancia: Crítica

Recursos afectados:

- MyCareLink Monitor, versiones 24950 y 24952
- CareLink Monitor, versión 2490C
- CareLink 2090 Programmer
- Amplia CRT-D, Claria CRT-D, Compia CRT-D, Concerto CRT-D, Concerto II CRT-D, Consulta CRT-D, Evera ICD, Maximo II CRT-D e ICD, Mirro ICD, Nayamed ND ICD, Primo ICD, Protecta ICD y CRT-D, Secura ICD, Virtuoso ICD, Virtuoso II ICD, Visia AF ICD y Viva CRT-D, todos los modelos.

Descripción:

Peter Morgan de Clever Security, Dave Singelée y Bart Preneel de KU Leuven, Eduard Marin anteriormente de KU Leuven, actualmente con la University of Birmingham, Flavio D. Garcia, Tom Chothia de la University of Birmingham y Rik Willems del University Hospital Gasthuisberg Leuvenha han reportado varias vulnerabilidades que afectan al protocolo de telemetría Conexus de Medtronic. Un atacante con acceso cercano a alguno de los productos afectados podría interferir, generar, modificar o interceptar la comunicación de radiofrecuencia (RF) del sistema de telemetría Conexus, afectando a la funcionalidad del producto y permitiendo el acceso a datos confidenciales transmitidos.

Solución:

Medtronic ha aplicado controles adicionales de monitorización y respuesta a usos inadecuados del protocolo por los dispositivos afectados. Además, está trabajando en nuevas mitigaciones que serán desplegadas con futuras actualizaciones. Medtronic también recomienda aplicar las siguientes medidas:

- Mantener control físico sobre los programadores y monitores.
- Utilizar sólo programadores, monitores y dispositivos implantables obtenidos directamente de su proveedor de productos de salud o de Medtronic.
- No conectar dispositivos inapropiados a los programadores y monitores mediante los puertos USB disponibles.
- Usar los programadores solo en ambientes físicamente controlados, como hospitales y clínicas autorizadas.
- Informar de cualquier comportamiento anómalo.

Detalle:

- El protocolo de telemetría Conexus no implementa autenticación y autorización. Un atacante con acceso de corto alcance a un producto afectado podría inyectar, reproducir, modificar e interceptar datos dentro de la comunicación de telemetría, así como cambiar la memoria en el dispositivo cardíaco implantado. Se ha reservado el identificador CVE-2019-6538 para esta vulnerabilidad.
- El protocolo de telemetría Conexus no implementa cifrado. Un atacante con acceso de corto alcance a un producto afectado podría escuchar las comunicaciones, incluida la transmisión de datos confidenciales. Se ha reservado el identificador CVE-2019-6540 para esta vulnerabilidad.

Etiquetas: 0day, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en dispositivos Phoenix Contact

Fecha de publicación: 26/03/2019

Importancia: Crítica

Recursos afectados:

- RAD-80211-XD (2885728)
- RAD-80211-XD/HP-BUS (2900047)
- FL NAT SMN 8TX-M (2702443)
- FL NAT SMN 8TX-M-DMG (2989352)
- FL NAT SMN 8TX (2989365)
- FL NAT SMCS 8TX (2989378)

Descripción:

El investigador de seguridad Maxim Rupp ha reportado a Phoenix Contact dos vulnerabilidades, una de severidad crítica y otra alta, que podrían permitir a un atacante no autorizado acceder al dispositivo o ejecutar comandos con privilegios de administrador.

Solución:

Phoenix Contact recomienda utilizar los dispositivos en redes controladas y protegidas con cortafuegos. En función del dispositivo afectado:

- Dispositivos RAD-80211-XD y RAD-80211-XD/HP-BUS: se encuentran sin soporte, por lo que no recibirán actualización que mitigue la vulnerabilidad. Phoenix Contact recomienda sustituir los dispositivos afectados.
- Dispositivos FL NAT: si un atacante lograse acceder exitosamente al dispositivo, se recomienda:
  - Cerrar la sesión de la interfaz web inmediatamente después de las tareas de administración.
  - Deshabilitar la interfaz web y utilizar la configuración de acceso a través de SNMP.

Detalle:

- La vulnerabilidad de severidad crítica se encuentra en la utilidad WebHMI. Cualquier usuario podría explotar la vulnerabilidad para ejecutar comandos en el dispositivo con privilegios de administrador. Se ha reservado el identificador CVE-2019-9743 para esta vulnerabilidad.
- La vulnerabilidad de criticidad alta se encuentra al iniciar sesión. La dirección IP origen es empleada como identificador de sesión y los usuarios que dispongan de la misma dirección IP podrían obtener acceso completo a la interfaz web. Se ha reservado el identificador CVE-2019-9744 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Falta de autenticación en controladores de iluminación de ENTTEC

Fecha de publicación: 27/03/2019

Importancia: Alta

Recursos afectados:

- Datagate MK2, todas las versiones de firmware anteriores a 70044_update_05032019-482.
- Storm 24, todas las versiones de firmware anteriores a 70050_update_05032019-482.
- Pixelator, todas las versiones de firmware anteriores a 70060_update_05032019-482.

Descripción:

El investigador Ankit Anubhav de NewSky Security ha reportado una vulnerabilidad de falta de autenticación en función crítica que afecta a los controladores de iluminación de ENTTEC y que podría permitir a un atacante remoto reiniciar el dispositivo dando lugar a una condición de denegación de servicio.

Solución:

ENTTEC recomienda a los usuarios actualizar a la versión de firmware de Marzo 2019 revB o porterior, la cual puede ser descargada siguiendo los siguientes enlaces:

- Datagate MK2 70044_update_05032019-482
- Storm 24 70050_update_05032019-482
- Pixelator 70060_update_05032019-482

Detalle:

- Un atacante sin autorización podría iniciar un reinicio del dispositivo, de manera remota, provocando una condición de denegación de servicio. Se ha asignado el identificador CVE-2019-6542 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Denegación de servicio en variadores de CA PowerFlex 525 de Rockwell Automation

Fecha de publicación: 29/03/2019

Importancia: Alta

Recursos afectados:

- Variadores de CA PowerFlex 525 con puerto EtherNet/IP embebido, versiones 5.001 y anteriores.

Nota: Los adaptadores 25-COMM-E2P Dual-Port EtherNet/IP, compatibles con los variadores de CA PowerFlex 525, no se ven afectados por esta vulnerabilidad.

Descripción:

El investigador Nicolas Merle, de Applied Risk, ha identificado una vulnerabilidad de consumo de recursos no controlados que afecta a los variadores de CA PowerFlex 525 de Rockwell Automation. Un atacante remoto podría agotar los recursos generando una condición de denegación de servicio o corromper la memoria.

Solución:

- Actualizar los dispositivos afectados con el firmware 5.002 o posterior.

Detalle:

- Un atacante remoto no autenticado podría, mediante él envió sucesivo de paquetes CIP específicos, agotar los recursos, generar una condición de denegación de servicios y/o corrupción de memoria en el producto afectado. Se ha reservado el identificador CVE-2018-19282 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Control de acceso inadecuado en WebAccess de Advantech

Fecha de publicación: 29/03/2019

Importancia: Crítica

Recursos afectados:

- WebAccess

Descripción:

El investigador Mat Powell, de Trend Micro Zero Day Initiative, ha reportado dos vulnerabilidades de control de acceso inadecuado, que afectan al software WebAccess de Advantech. Un atacante remoto podría ejecutar código arbitrario en el dispositivo sin estar autenticado.

Solución:

- No se ha publicado ninguna solución para estas vulnerabilidades. Se aconseja restringir la interacción únicamente a máquinas de confianza. Solo se debe permitir la comunicación con WebAccess a clientes y servidores relacionados de forma legítima en el proceso.

Detalle:

- Se ha detectado una falta de validación de la cadena de texto proporcionada por el usuario, en los servicios *spchapi.exe* y *tv_enua.exe*, antes de utilizarse para ejecutar una llamada al sistema. Un atacante remoto no autenticado podría ejecutar código arbitrario en el contexto de Administrador.

Etiquetas: 0day, Vulnerabilidad