Boletín de diciembre de 2018

Avisos de Sistemas de Control Industrial

Autenticación inadecuada en Controladores Access Easy de Bosch

Fecha de publicación: 04/12/2018

Importancia: Media

Recursos afectados:

- Controlador Access Easy, versión 2.1

Descripción:

El investigador independiente Maxim Rupp ha identificado una vulnerabilidad de autenticación inadecuada en los controladores Access Easy de Bosch que podría permitir a un atacante el acceso a los recursos del dispositivo.

Solución:

Actualizar a la versión 2.1.9.3 del firmware.

Detalle:

- El dispositivo Access Easy usa el servicio gSOAP para recuperar datos en tiempo real y el estado del sensor para los navegadores de los clientes. Un atacante, conociendo la última conexión URL de SOAP, podría acceder al dispositivo sin necesidad de autorización de usuario y usar la interfaz del dispositivo.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad Cross-site Scripting en SCADA Webserver de SpiderControl

Fecha de publicación: 05/12/2018

Importancia: Media

Recursos afectados:

- SCADA Webserver, versiones anteriores a 2.03.0001

Descripción:

El investigador independiente Ismail Bulbul ha reportado una vulnerabilidad de tipo *Reflected cross-site Scripting* (RXSS) que afecta a los equipos SCADA Webserver de SpiderControl.

Solución:

- Actualizar SCADA Webserver a la versión 2.03.0001

Detalle:

- Las secuencias de comandos entre sitios reflejados (no persistentes) podrían permitir que un atacante envíe una URL especialmente diseñada con contenido JavaScript, para que se refleje desde la aplicación web al navegador de la víctima. Se ha asignado el identificador CVE-2018-18991 para esta vulnerabilidad.

Etiquetas: Actualización, Navegador, SCADA, Vulnerabilidad

Múltiples vulnerabilidades en CX-One de Omron

Fecha de publicación: 05/12/2018

Importancia: Media

Recursos afectados:

- CX-One, versiones 4.42 y anteriores, incluyendo las siguientes aplicaciones:
  - CX-Programmer, versiones 9.66 y anteriores.
  - CX-Server, versiones 5.0.23 y anteriores.

Descripción:

El investigador Esteban Ruiz de Source Incite, trabajando con Zero Day Initiative de Trend Micro, ha identificado varias vulnerabilidades de desbordamiento de búfer y de uso de memoria previamente liberada en productos CX-One de Omron. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante ejecutar código bajo los privilegios de la aplicación.

Solución:

Omron ha publicado nuevas versiones que solucionan estas vulnerabilidades:

- CX-Programmer, versión 9.70
- Módulo común, incluyendo CX-Server, versión 5.0.24

Detalle:

- Un potencial atacante podría utilizar un fichero de proyecto especialmente manipulado para sobrepasar el tamaño del búfer y conseguir la ejecución de código bajo los privilegios de la aplicación, provocando un desbordamiento de búfer basado en pila (*stack based buffer overflow*). Se ha asignado el identificador CVE-2018-18993 para esta vulnerabilidad.
- Mediante la utilización de un fichero específicamente modificado, un potencial atacante podría explotar y ejecutar código bajo los privilegios de la aplicación, aprovechando un fallo en la comprobación de las referencias a memoria liberada. Se ha asignado el identificador CVE-2018-18989 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Allen-Bradley PowerMonitor 1000 de Rockwell Automation

Fecha de publicación: 05/12/2018

Importancia: Alta

Recursos afectados:

- PowerMonitor 1000

Descripción:

El investigador Luca Chiou ha identificado varias vulnerabilidades del tipo acceso de control inadecuado y cross-site scripting en el producto PowerMonitor 1000 de Allen-Bradley. Un potencial atacante podría crear nuevos usuarios en el dispositivo o inyectar código XSS.

Solución:

No hay disponible solución para estas vulnerabilidades.

Detalle:

- El control de acceso inadecuado podria permitir a un atacante remoto usar el proxy para habilitar funciones del dispositivo lo que podría permitir crear usuarios nuevos. Se ha asignado el CVE-2018-19616 a esta vulnerabilidad.
- Un atacante podría inyectar código XSS en un parámetro de la cuenta del usuario que almacenarse en la base de datos.

Etiquetas: 0day, Vulnerabilidad

Restricción insuficiente en referencias de entidad externa XML en Proficy GDS de GE

Fecha de publicación: 07/12/2018

Importancia: Alta

Recursos afectados:

Cimplicity versiones 9.0 R2, 9.5 y 10.0

Descripción:

El investigador Vladimir Dashchenko de Kaspersky Lab ha reportado una vulnerabilidad del tipo restricción insuficiente en referencias de entidad externa XML en Proficy GDS de General Electric que podría permitir a un atacante iniciar una sesión OPC UA y recuperar algún archivo del sistema objetivo.

Solución:

- GE aconseja a los clientes actualizar a la versión 2.1 o superior.

Detalle:

- La restricción inadecuada de referencias XXE (XML External Entity) podría permitir, mediante inyecciones XXE, llegar a una ruta dentro del servidor Proficy, iniciar una sesión de OPC UA y recuperar archivos del sistema objetivo. Se ha asignado el identificador CVE-2018-15362 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Cifrado débil en aplicación Android HealthSuite Health de Philips

Fecha de publicación: 07/12/2018

Importancia: Baja

Recursos afectados:

- Aplicación Android HealthSuite Health, todas las versiones.

Descripción:

Un investigador anónimo ha reportado esta vulnerabilidad de tipo cifrado débil en las comunicaciones de la aplicación Android HealthSuite Health perteneciente a Philips que podría permitir a un atacante con acceso físico al dispositivo, afectar a la confidencialidad e integridad de la aplicación.

Solución:

- La nueva versión de la aplicación Android que solventará la vulnerabilidad estará disponible durante el primer trimestre de 2019.
- Como mitigación temporal de la vulnerabilidad, Philips recomienda seguir las siguientes pautas:
  - Los dispositivos móviles rooteados o a los que se les ha aplicado un jail-break, permiten modificar configuraciones fuera de unas restricciones preestablecidas por el sistema. Es por esta razón que las limitaciones impuestas en las aplicaciones desarrolladas como la afectada por el proveedor, pueden no tener el efecto deseado. El salto de restricciones aplicando un rooteo o un jail-break podría afectar al rendimiento de las aplicaciones, debilitar la seguridad del dispositivo y exponer a los usuarios existentes en el sistema, en este caso Android, a riesgos adicionales.

Detalle:

- El software afectado utiliza un cifrado que no se considera robusto. Un potencial atacante con acceso físico al dispositivo podría afectar a la confidencialidad e integridad del producto. Se ha asignado el identificador CVE-2018-19001 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en Eurotherm GUIcon de Schneider Electric

Fecha de publicación: 07/12/2018

Importancia: Alta

Recursos afectados:

- Eurotherm GUIcon Versión 2.0 Gold Build 683.0

Descripción:

Los investigadores mdm y rgod de 9SG Security Team han reportado a Schneider Electric varias vulnerabilidades del tipo uso de tipos de datos incompatibles y desbordamiento de búfer que podrían permitir a un atacante la ejecución remota de código.

Solución:

- Actualizar a GUIcon Version 2.0 Software Package (Gold Build 683.003)

Detalle:

- Una vulnerabilidad de uso de tipos de datos incompatibles en pcwin.dll a la hora de procesar ficheros GD1 podría permitir a un atacante la ejecución remota de código. Se ha asignado el identificador CVE-2018-7813 para esta vulnerabilidad.
- Una vulnerabilidad de desbordamiento de búfer basado en la pila a la hora de procesar ficheros GD1 podría permitir a un potencial atacante la ejecución remota de código. Se ha asignado el identificador CVE-2018-7814 para esta vulnerabilidad.
- Una vulnerabilidad de uso de tipos de datos incompatibles en c3core.dll a la hora de procesar ficheros GD1 podría permitir a un atacante la ejecución remota de código. Se ha asignado el identificador CVE-2018-7815 para esta vulnerabilidad.

Etiquetas: Schneider Electric, Vulnerabilidad

Vulnerabilidad en xComfort de Eaton

Fecha de publicación: 10/12/2018

Importancia: Alta

Recursos afectados:

- Controlador de casas inteligentes (*Smart Home Controller*, SHC) xComfort, versión SHC-7.5-2.3.2 y anteriores.

Descripción:

Eaton ha sido informado de una vulnerabilidad que afecta al controlador de casas inteligentes (SHC) xComfort.

Solución:

Eaton ha publicado la versión de *firmware* SHC-7.5-2.3.3 que soluciona esta vulnerabilidad.

Detalle:

- No se dispone de más información por el momento.

Etiquetas: Actualización, Privacidad, Vulnerabilidad

Múltiples vulnerabilidades en productos Siemens

Fecha de publicación: 11/12/2018

Importancia: Crítica

Recursos afectados:

- SINUMERIK 808D V4.7, todas las versiones.
- SINUMERIK 808D V4.8, todas las versiones.
- SINUMERIK 828D V4.7, todas las versiones anteriores a la V4.7 SP6 HF1.
- SINUMERIK 840D sl V4.7, todas las versiones anteriores a la V4.7 SP6 HF5.
- SINUMERIK 840D sl V4.8, todas las versiones anteriores a la V4.8 SP3.
- SINAMICS PERFECT HARMONY GH180, con drivers MLFB 6SR32, MLFB 6SR52, MLFB 6SR42 con opción A30 y MLFB 6SR325.
- TIM 1531 IRC, todas las versiones anteriores a la V2.0.

Descripción:

Los investigadores de Kaspersky Lab y McAfee Corporation, Anton Kalinin, Danila Parnishchev, Dmitry Sklyar, Gleb Gritsai, Kirill Nesterov, Radu Motspan y Sergey Sidorov han coordinado con Siemens el tratamiento de varias vulnerabilidades de tipo de envío de falta de control en permisos de ficheros, escalada de privilegios, desbordamiento de búfer, autenticación inadecuada y falta de control en llamadas ioctl que podrían permitir a un atacante provocar denegaciones de servicio, ejecutar código malicioso, realizar escaladas de privilegios u originar un malfuncionamiento de los dispositivos afectados.

Solución:

- Para las vulnerabilidades CVE-2018-11457, CVE-2018-11458, CVE-2018-11459, CVE-2018-11460, CVE-2018-11461, CVE-2018-11462, CVE-2018-11463, CVE-2018-11464, CVE-2018-11465, CVE-2018-11466, Siemens recomienda:
  - Revisar y restaurar las configuraciones por defecto (puertos 4842/tcp y 5900/tcp bloqueados) del cortafuegos para los puertos X130.
  - Restringir el acceso a los productos afectados solo a personal autorizado con los mínimos permisos posibles.
  - Aplicar el concepto de protección de celdas.
  - Usar VPN para la protección de las comunicaciones de red entre celdas.
  - Aplicar el concepto de defensa en profundidad.
- CVE-2018-6690:
  - Proteger el acceso local al disco.
  - Asegurarse de que los dispositivos de almacenamiento USB están en blanco y libres de malware antes de conectarlos al disco.
  - Aplicar el concepto de protección de celdas e implementar defensa en profundidad.
- CVE-2018-13816:
  - Restringir el acceso al puerto 102/tcp a direcciones IP de confianza.
  - Actualizar a la versión de firmware V2.0 (y reiniciar la estación TIM de ingeniería).
- Para más información, consultar los siguientes enlaces:
  - https://www.siemens.com/cert/operational-guidelines-industrial-security.
  - https://www.siemens.com/industrialsecurity.

Detalle:

Un usuario malintencionado podría aprovechar alguna de estas vulnerabilidades del tipo:

- Envío de paquetes especialmente diseñados.
- Falta de control en permisos de ficheros.
- Falta de control en permisos de ficheros CRAMFS.
- Escalada de privilegios.
- Envío de paquetes especialmente diseñados.
- Desbordamiento de búfer.
- Denegación de servicio en servidor VNC.
- Falta de control en llamadas ioctl.
- Envío de paquetes especialmente diseñados.
- Ejecución de código.
- Autenticación inadecuada.

Se han reservado los identificadores CVE-2018-11457, CVE-2018-11458, CVE-2018-11459, CVE-2018-11460, CVE-2018-11461, CVE-2018-11462, CVE-2018-11463, CVE-2018-11464, CVE-2018-11465, CVE-2018-11466 y CVE-2018-13816, y asignado CVE-2018-11490 para estas vulnerabilidades.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Vulnerabilidad cross-site scripting en PI Vision de OSIsoft

Fecha de publicación: 12/12/2018

Importancia: Media

Recursos afectados:

- PI Vision 2017
- PI Vision 2017 R2

Descripción:

OSIsoft ha identificado una vulnerabilidad de tipo cross-site scripting que afecta a sus productos PI Vision y podrían permitir a un atacante remoto modificar diferentes atributos de la página web y de la aplicación PI Visión.

Solución:

- OSIsoft recomienda actualizar a la versión PI Vision 2017 R2 SP1 para solucionar esta vulnerabilidad.

Detalle:

- El producto afectado utiliza código JavaScript en elementos y atributos AF, un atacante remoto podría leer y modificar el contenido de la página web de PI VIsion y los datos relacionados con la aplicación PI Vision en el navegador de la víctima. Requiere la habilidad de que un usuario de AF autorizado almacene JavaScript en elementos y atributos de AF.

Etiquetas: Actualización, Vulnerabilidad

Desbordamiento de búfer en cámaras IP de Bosch

Fecha de publicación: 13/12/2018

Importancia: Crítica

Recursos afectados:

- Common Product Platform 7.3 (CPP7.3)
  - AUTODOME IP 4000i, 5000i, starlight 5000i (IR) y starlight 7000i
  - DINION IP bullet 4000i, 5000i y 6000i
  - FLEXIDOME IP 4000i y 5000i
  - MIC IP starlight 7000i y fusion 9000i
- CPP7:
  - DINION IP starlight 6000 y 7000
  - DINION IP thermal 8000
  - FLEXIDOME IP starlight 6000 y 7000
- CPP6:
  - DINION IP starlight 8000 12MP y ultra 8000 12MP
  - FLEXIDOME IP panoramic 6000 12MP 180, 360, 180 IVA y 360 IVA
  - FLEXIDOME IP panoramic 7000 12MP 180, 360, 180 IVA y 360 IVA
  - AVIOTEC IP starlight 8000
- CPP4:
  - AUTODOME IP 4000 HD, 5000 HD, 5000 IR y serie 7000
  - DINION HD 1080p, 1080p HDR, 720p
  - DINION imager 9000 HD
  - DINION IP bullet 4000, 4000 HD, 5000, 5000 HD, 5000 MP y starlight 7000 HD
  - EXTEGRA IP dynamic 9000 y starlight 9000
  - FLEXIDOME corner 9000 MP
  - FLEXIDOME HD 1080p, 1080p HDR y 720p
  - FLEXIDOME IP panoramic 5000
  - FLEXIDOME IP indoor 5000 HD, 5000 MP, 4000 HD, 4000 IR,
  - FLEXIDOME IP outdoor 4000 HD, 4000 IR, 5000 HD, 5000 MP
  - FLEXIDOME IP micro 5000 HD, 5000 MP, 2000 HD y 2000 IP
  - IP bullet 4000 HD y 5000 HD
  - IP micro 2000 y 2000 HD
  - MIC IP dynamic 7000 y starlight 7000
  - TINYON IP 2000 family
  - Vandal-proof FLEXIDOME HD 1080p, 1080p HDR y 720p

Descripción:

- Un investigador independiente ha identificado una vulnerabilidad de desbordamiento de búfer en cámaras IP de Bosch que podría permitir a un atacante ejecutar código remoto en los dispositivos afectados.

Solución:

- Bosh recomienda actualizar el firmware de los dispositivos a las siguientes actualizaciones:
  - Las versiones de firmware que solucionan esta vulnerabilidad son 6.51.0028, 6.50.0133, 6.44.0027 para todos los CPP
- Bosch también aconseja una versión concreta dependiendo de la versión de BVMS (Bosch Video Management System) utilizada:
  - BVMS 7.0, 7.5, y 8.0: versión 6.44.0027 para todos los CPP
  - BVMS 9.0: versión 6.51.0028 para todos los CPP

Detalle:

- Un atacante remoto podría provocar un desbordamiento de búfer que le permitiría ejecutar código y acceder a usuarios y contraseñas, pudiendo activar opciones o bloquear el dispositivo afectado. Se ha reservado el identificador CVE-2018-19036 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Inyección de comandos de sistema operativo en cámaras IP E2 de Geutebrück GmbH

Fecha de publicación: 14/12/2018

Importancia: Alta

Recursos afectados:

- Cámaras serie E2, versiones anteriores 1.12.0.25

Descripción:

- Un investigador Davy Douhine de RandoriSec ha identificado una vulnerabilidad de inyección de comandos de sistema operativo en las cámaras IP de la serie E2 de Geutebrück GmbH que podría permitir a un atacante remoto ejecutar comandos como usuario ? root?.

Solución:

- Geutebrück GmbH ha publicado la versión de firmware 1.12.0.25

Detalle:

- La configuración de DDNS en el panel de configuración de la cámara podría permitir a un atacante remoto ejecutar comandos como usuario ?root?. Se ha reservado el identificador CVE-2018-19007 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Falta de cifrado de datos sensibles en productos CareLink y Encore de Medtronic

Fecha de publicación: 14/12/2018

Importancia: Media

Recursos afectados:

- CareLink 9790 Programmer, todas las versiones.
- CareLink 2090 Programmer, todas las versiones.
- 29901 Encore Programmer, todas las versiones.

Descripción:

Los investigadores Billy Rios y Jonathan Butts de Whitescope LLC han identificado una vulnerabilidad de falta de cifrado de datos sensibles que pueden contener información médica protegida o información personal identificable, esto podría permitir a un atacante con acceso físico al dispositivo consultar esta información.

Solución:

- El dispositivo CareLink 9790 Programmer está obsoleto, Medtronic recomienda que ya no se utilice más. Además, la compañía recomienda para CareLink 2090 Programmer y 29901 Encore Programmer que se mantenga la información médica y personal almacenada en estos dispositivos el menor tiempo posible. También ha publicado un boletín de seguridad relacionado con este aviso.

Detalle:

- Un atacante remoto podría aprovecharse de la falta de cifrado en datos sensibles para conseguir información médica y personal de los usuarios almacenados en los distintos dispositivos. Se ha reservado el identificador CVE-2018-18984 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, Vulnerabilidad

Salto de ruta en Mark VIe de GE

Fecha de publicación: 14/12/2018

Importancia: Alta

Recursos afectados:

- Mark VIe, versiones desde la 03.03.28C hasta la 05.02.04C
- EX2100e, EX2100e_Reg y LS2100e, versiones anteriores a la v04.09.00C

Descripción:

El investigador Can Demirel de Biznet Bilisim ha reportado una vulnerabilidad de tipo salto de ruta que afecta a los dispositivos DCS Mark Vie de GE que podría permitir a un atacante acceder a datos del sistema, dando lugar a un escalado de privilegios y a un acceso sin autorización al controlador.

Solución:

GE ha solucionado esta vulnerabilidad en la versión actual del software ControlST, la cual se encuentra disponible para usuarios

registrados en el portal de GE Power ServiceNow

Detalle:

- Un potencial atacante podría obtener acceso a información restringida aprovechando un fallo de restricción de salto de ruta. Se ha asignado el identificador CVE-2018-19003 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en dispositivos GATE de ABB

Fecha de publicación: 17/12/2018

Importancia: Crítica

Recursos afectados:

- GATE-E2, todas las versiones.
- GATE-E1, todas las versiones.

Descripción:

El investigador Nelson Berg de Applied Risk ha reportado dos vulnerabilidades de tipo *Cross-Site Scripting* (XSS) y falta de soporte de autenticación que afecta a los dispositivos GATE de ABB. Un potencial atacante podría dejar los dispositivos inaccesibles o realizar una inyección de código.

Solución:

Los productos afectados se encuentran fuera de su ciclo de vida útil, por lo que ABB no va a publicar nuevas versiones de firmware que solucionen estas vulnerabilidades.

No obstante, ABB ha comunicado a todos los usuarios, vía correo electrónico, instrucciones para configurar de manera segura estos dispositivos.

Además, ABB recomienda proteger los dispositivos de accesos directos por personal no autorizado, no disponer de conexiones directas a Internet, separar estos equipos de otros en redes controladas por cortafuegos y exponer el mínimo número de puertos.

Detalle:

- Un atacante podría realizar un *Cross-Site Scripting* y dejar los dispositivos inaccesibles cambiando la configuración del producto o reiniciando de manera continua el producto. Se ha reservado el identificador CVE-2018-18997 para esta vulnerabilidad.
- Un atacante remoto podría inyectar *scripts* en el lado del cliente en la página web del producto y comprometer el navegador de los usuarios conectados a la interfaz web del producto debido a una falta de soporte en la autenticación. Se ha reservado el identificador CVE-2018-18995 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Vulnerabilidad en XP503 de Eaton

Fecha de publicación: 17/12/2018

Importancia: Media

Recursos afectados:

- XP503 Visual Designer.
- XP503 Galileo.

Descripción:

Eaton ha identificado una vulnerabilidad que afecta al Panel PC XP503 causada por el uso de Windows Embedded Standard 7.

Solución:

Todavía no se ha publicado una solución para esta vulnerabilidad.

- Eaton ha programado una nueva versión para los dispositivos XP503 para el primer trimestre de 2019.

Detalle:

- No se dispone de más información por el momento.

Etiquetas: Vulnerabilidad

Validación incorrecta de entradas en WebAccess/SCADA de Advantech

Fecha de publicación: 19/12/2018

Importancia: Alta

Recursos afectados:

- WebAccess/SCADA, versión 8.32 instalada en Windows 2008 R2 SP1

Descripción:

El investigador Jacob Baines de Tenable Network Security ha reportado una vulnerabilidad de tipo validación incorrecta de entradas que afectan al software SCADA WebAccess/SCADA de Advantech.

Solución:

- Advantech ha publicado la actualización 8.3.4 que soluciona esta vulnerabilidad.

Detalle:

- Una validación incorrecta de las entradas podría permitir a un atacante remoto causar desbordamiento de búfer en la pila. Se ha reservado el código CVE-2018-18999 para esta vulnerabilidad.

Etiquetas: Actualización, SCADA, Vulnerabilidad

Múltiples vulnerabilidades en productos CODESYS de 3S-Smart Software Solutions GmbH

Fecha de publicación: 19/12/2018

Importancia: Crítica

Recursos afectados:

- CODESYS Control para BeagleBone, emPC-A/iMX6, IOT2000, Linux, PFC100, PFC200 y Raspberry Pi.
- CODESYS Control RTE V3 y RTE V3 para Beckhoff CX.
- CODESYS Control Win V3 (también parte de la configuración de CODESYS).
- CODESYS Control V3 Runtime System Toolkit.
- CODESYS V3 Simulation Runtime (parte del CODESYS Development System).
- CODESYS V3 Embedded Target Visu Toolkit.
- CODESYS V3 Remote Target Visu Toolkit.
- CODESYS V3 Safety SIL2.
- CODESYS V3 Development System.
- CODESYS Gateway V3.
- CODESYS HMI V3.
- CODESYS OPC Server V3.
- CODESYS PLCHandler SDK.

3S-Smart Software Solutions GmbH informa de que la vulnerabilidad identificada con CVE-2018-10612 afecta a todas las variantes de los productos CODESYS Control V3 que contienen los componentes *CmpSecureChannel* o *CmpUserMgr* anteriores a la versión 3.5.14.0, independientemente del tipo de CPU o sistema operativo

Descripción:

Los investigadores Alexander Nochvay y Yury Serdyuk de Kaspersky Lab han reportado varias vulnerabilidades de tipo uso de valores insuficientemente aleatorios, restricción inadecuada del canal de comunicación y control de accesos inadecuado que afectan a los productos CODESYS V3 y CODESYS control V3 de 3S-Smart Software Solutions GmbH. Un potencial atacante remoto podría ocultar el origen de paquetes maliciosos, explotar una debilidad en los valores aleatorios afectando a la confidencialidad e integridad de los datos o conseguir acceso no autorizado al dispositivo y la divulgación de información sensible, incluidas las credenciales de usuario.

Solución:

- 3-S Smart Software Solutions GmbH recomienda actualizar a la versión 3.5.14.0 o superior desde su centro de descargas. Además, también recomienda activar el control de CODESYS para la gestión de usuarios online y el cifrado de las comunicaciones.

Detalle:

- La utilización de valores insuficientemente aleatorios afecta a la confidencialidad e integridad de los datos almacenados en el dispositivo. Se ha reservado el identificador CVE-2018-20025 para esta vulnerabilidad.
- La restricción inadecuada del canal de comunicación permitiría falsificar el origen de los paquetes en la comunicación. Se ha reservado el identificador CVE-2018-20026 para esta vulnerabilidad.
- La gestión inadecuada de acceso de los usuarios y el cifrado de la comunicación deshabilitado por defecto permitiría a un potencial atacante acceder al dispositivo y a información sensible, incluyendo las credenciales de los usuarios. Se ha reservado el identificador CVE-2018-10612 para esta vulnerabilidad.
- Exposición de información sensible.
- Denegación de servicio.
- Denegación de servicio remota.

Etiquetas: Comunicaciones, Vulnerabilidad

Vulnerabilidad de redirección de URL en Power Monitoring Expert de Schneider Electric

Fecha de publicación: 20/12/2018

Importancia: Alta

Recursos afectados:

- EcoStruxure™ Power Monitoring Expert (PME), versiones 8.2 (todas las ediciones) y 9.0

- EcoStruxure™ Energy Expert (anteriormente denominado Power Manager), versiones 1.3 y 2.0
- EcoStruxure™ Power SCADA Operation (PSO) Advanced Reports y Dashboards Module, versiones 8.2 y 9.0

Descripción:

El investigador Donato Onofri, de Business Integration Partners S.p.A, ha reportado una vulnerabilidad de tipo redirección de URL con la que un atacante remoto podría causar un ataque de *phishing*, redireccionando a un sitio malicioso.

Solución:

- Para PME v8.2, Energy Expert v1.3 y PSO v8.2 Advance Reports y Dashboard Module, descargar PME 8.2 CU3.
- Para PME v9.0, Energy Expert v2.0 y PSO v9.0 Advance Reports y Dashboard Module, descargar CU1 18328.01.

Detalle:

- Un atacante remoto podría causar un ataque de *phishing*, redireccionando al usuario a un sitio malicioso. Se ha asignado el identificador CVE-2018-7797 para esta vulnerabilidad.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Validación incorrecta de entrada en Cscape de Horner Automation

Fecha de publicación: 21/12/2018

Importancia: Media

Recursos afectados:

- Cscape versión 9.80.75.3 SP3 y anteriores.

Descripción:

Los investigadores rgod y mdm, de 9SG Security Team, en colaboración con Zero Day Initiative de Trend Micro, han reportado una vulnerabilidad de tipo validación incorrecta de entrada al NCCIC.

Solución:

- Horner Automation recomienda actualizar a la última versión de Cscape disponible (versión 9.80 SP4) para solventar la vulnerabilidad, disponible para su descarga en América y resto del mundo.

Detalle:

- Un atacante podría crear un archivo de POC especialmente diseñado para ser procesado por el software Cscape, que carece de mecanismos para la validación de estos archivos cuando son introducidos por un usuario. Este hecho permitiría al atacante acceder a información confidencial y ejecutar de forma remota código arbitrario. Se ha asignado el identificador CVE-2018-19005 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Desbordamiento de búfer en FactoryTalk Services Platform de Rockwell Automation

Fecha de publicación: 21/12/2018

Importancia: Alta

Recursos afectados:

- FactoryTalk Services Platform, versión 2.90 y anteriores.

Descripción:

- El investigador Andrey Zhukov ha reportado una vulnerabilidad de tipo desbordamiento de búfer.

Solución:

- Rockwell recomienda actualizar a la última versión disponible en su centro de descargas.

Detalle:

- Un atacante remoto sin autenticar podría enviar numerosos paquetes especialmente diseñados a los puertos de servicio, provocando un consumo de la memoria que podría originar una condición parcial o completa de denegación de servicio a los servicios afectados. Se ha reservado el identificador CVE-2018-18981 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Denegación de servicio en el controlador Vnet/IP Open Communication de Yokogawa

Fecha de publicación: 21/12/2018

Importancia: Alta

Recursos afectados:

- CENTUM
  - CS 3000 y CS 3000 Entry Class, versiones desde R3.05.00 hasta R3.09.50
  - VP y VP Entry Class, versiones desde R4.01.00 hasta R6.03.10
- Exaopc, versiones desde R3.10.00 hasta R3.75.00
- PRM, versiones desde R2.06.00 hasta R3.31.00
- ProSafe-RS, versiones desde R1.02.00 hasta R4.02.00
- FAST/TOOLS, versiones desde R9.02.00 hasta R10.02.00
- B/M9000 VP, versiones desde R6.03.01 hasta R8.01.90

Descripción:

Yokogawa ha identificado una vulnerabilidad de denegación de servicio que afecta su controlador Vnet/IP Open Communication.

Solución:

Para los siguientes productos no hay solución disponible, ya que Yokogawa indica que se encuentran descatalogados y recomienda renovar a una versión más reciente:

- CENTUM CS 3000 y CS 3000 Entry Class, versiones desde R3.05.00 hasta R3.09.50
- CENTUM VP y VP Entry Class, todas las versiones de la serie R4
- Exaopc, versiones desde R3.10.00 hasta R3.60.00
- PRM, versiones desde R2.06.00 hasta R3.04.00
- ProSafe-RS, todas las versiones de las series R1 y R2

Para los siguientes productos Yokogawa recomienda actualizar el controlador Vnet/IP Open Communication a la versión de software R10.01.08:

- CENTUM VP y VP Entry Class, todas las versiones de la series R5 y versiones anteriores a R6.03.10 en la serie R6
- Exaopc, versiones desde R3.70.00 hasta R3.75.00 (la vulnerabilidad fue corregida en la versión R3.76.00)
- PRM, versiones desde R3.05.00 hasta R3.31.00 (la vulnerabilidad fue corregida en la versión R4.01.00)
- ProSafe-RS, todas las versiones de la serie R3 y versiones anteriores a R4.02.00 en la serie R4 (la vulnerabilidad fue corregida en la versión R4.03.00)
- FAST/TOOLS, versiones desde R9.02.00 hasta R9.05.00 y anteriores a R10.02.00 en la serie R10 (la vulnerabilidad fue corregida en la versión R10.03.00)
- B/M9000 VP, versiones desde R6.03.01 hasta R8.01.90. Este dispositivo no se encuentra afectado por la vulnerabilidad si no se encuentra instalado CENTUM VP en el mismo PC. Si CENTUM VP instalado necesita actualizarse, actualizar B/M9000 VP a una revisión adecuada.

Detalle:

- Una vulnerabilidad de denegación de servicio podría permitir a un atacante remoto detener la función de comunicación del controlador Vnet/IP Open Communication.

Etiquetas: Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos de Schneider Electric

Fecha de publicación: 26/12/2018

Importancia: Crítica

Recursos afectados:

- Todas las versiones de PowerSuite2 (VW3A8104 & Patches)
- IIoT Monitor, versión 3.1.38
- Pro-Face GP-Pro EX, versión 4.08 y anteriores
- EVLink Parking, versión 3.2.0-12_v1 y anteriores
- Todas las versiones de Foxboro DCS y Foxboro Evo
- IA Series en versiones anteriores a Foxboro DCS Control Core Service 9.4
- FoxView versión 10.5

Descripción:

Los investigadores Vahagn Vardanyan, Rgo (Zero Day Initiative), Yu Quiang (ADLab de Venustech) y Vladimir Kononovich, Vyacheslav Moskvin e Ilya Karpov (Positive Technologies), en colaboración con Schneider Electric, han reportado varias vulnerabilidades de tipo desbordamiento de búfer, gestión inadecuada de directorios restringidos, restricción incorrecta de XML, carga de archivos errónea, validación incorrecta de entrada, inyección SQL, administración inadecuada de credenciales e inyección de código, que podrían permitir a un atacante ejecutar código malicioso, obtener accesos sin permiso a los dispositivos, divulgar y modificar de forma no autorizada las contraseñas o acceder a archivos.

Solución:

- Para la vulnerabilidad en PowerSuite 2, Schneider recomienda:
  - Para los modelos ATV11, ATV28, ATV38, ATV58, ATV58F o Lexium05: conectar el ordenador detrás de un cortafuegos que impida cualquier conexión remota en el puerto 27698.
  - Para el resto de modelos, seguir las instrucciones del punto 2 de la sección *Remediation*.
- Para las vulnerabilidades en IIoT Monitor: contactar con el centro de atención al cliente de Schneider Electric.
- Para la vulnerabilidad en Pro-Face GP-Pro EX: descargar la versión 4.08.200
- Para las vulnerabilidades en EVLink Parking: descargar el *fix*.
- Para la vulnerabilidad FoxView HMI SCADA: actualizar Foxboro DCS Control Core Service 9.4 y Foxview 10.5 a versiones superiores.

Detalle:

Un atacante podría aprovechar alguna de las vulnerabilidades para tomar el control del dispositivo o provocar un funcionamiento erróneo del mismo:

- Desbordamiento de búfer.
- Gestión inadecuada de directorios restringidos.
- Carga de archivos inadecuada.
- Restricción inadecuada de XML.
- Validación incorrecta de entradas.
- Inyección de código.
- Inyección SQL.
- Administración inadecuada de credenciales.

Se han asignado los identificadores CVE-2018-7796, CVE-2018-7835, CVE-2018-7836, CVE-2018-7837, CVE-2018-7832, CVE-2018-7800, CVE-2018-7801, CVE-2018-7802 y CVE-2018-7793 para estas vulnerabilidades.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Corrupción de memoria en Zelio Soft de Schneider Electric

Fecha de publicación: 28/12/2018

Importancia: Alta

Recursos afectados:

- Zelio Soft 2, versión 5.1 y anteriores.

Descripción:

Los investigadores mdm y rgod, de 9SG Security Team, han detectado una vulnerabilidad de uso de memoria previamente liberada (*use after free*) que permitiría a un atacante la ejecución remota de código.

Solución:

Schneider Electric ha corregido esta vulnerabilidad en ZelioSoft2 v5.2

Detalle:

- Mediante la utilización de un fichero específicamente modificado, un atacante podría llegar a ejecutar código de manera remota, al aprovechar un fallo en la comprobación de las referencias a la memoria liberada. Se ha reservado el identificador CVE-2018-7817 para esta vulnerabilidad.

Etiquetas: Schneider Electric, Vulnerabilidad