Boletín de Julio de 2018

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en dispositivos SICLOCK TC de Siemens

Fecha de publicación: 04/07/2018

Importancia: Crítica

Recursos afectados:

- SICLOCK TC100, todas las versiones.
- SICLOCK TC400, todas las versiones.

Descripción:

Siemens ha identificado múltiples vulnerabilidades relacionadas con dispositivos SICLOCK TC que permitirían a un atacante remoto generar denegaciones de servicio, realizar una evasión de autenticación, ejecutar código arbitrario y modificar el firmware, tanto del dispositivo, como del cliente que permite la administración del mismo.

Solución:

Siemens recomienda a sus clientes seguir los siguientes pasos para mitigar las vulnerabilidades y reducir el riesgo:

- Utilizar fuentes de tiempo redundantes e implementar una verificación de las mismas para tener un control de la información del tiempo.
- Proteger el acceso a la red donde se encuentran los dispositivos afectados con cortafuegos para reducir el riesgo de exposición.
- Se recomienda filtrar todos los puertos, excepto los necesarios para la sincronización de tiempo.
  - Si la sincronización de tiempo se realiza mediante el protocolo NTP, se debería abrir el puerto 123/UDP en el cortafuegos.
  - Si se realiza utilizando la sincronización de tiempo SIMATIC, deberían abrirse los puertos 22223/UDP y el puerto 22224/UDP en el cortafuegos.
- Para la configuración de éstos parÃimetros se aconseja el uso de una conexión directa con el dispositivo SICLOCK TC.
- Aplicar el concepto de Defensa en Profundidad: https://www.siemens.com/cert/operational-guidelines-industrial-security

Detalle:

- Denegación de servicio: Un atacante remoto con acceso al dispositivo podría causar una condición de denegación de servicio enviando determinados paquetes al dispositivo, causando reinicios e impactando en la funcionalidad del dispositivo afectado. La funcionalidad se recupera cuando se completa la sincronización de tiempo mediante GPS o NTP. Se ha reservado el identificador CVE-2018-4851 para esta vulnerabilidad.
- Evasión de autenticación: Un atacante remoto podría evadir la autenticación si dispone del conocimiento suficiente del dispositivo atacado. La explotación exitosa de esta vulnerabilidad permitiría la lectura y modificación de la configuración del dispositivo. Se ha reservado el identificador CVE-2018-4852 para esta vulnerabilidad.
- Ejecución de código arbitrario: Un atacante remoto con acceso al puerto 69/UDP podría modificar el firmware del dispositivo y conseguir la ejecución de código arbitrario. La explotación de esta vulnerabilidad no requiere de interacción del usuario. Se ha reservado el identificador CVE-2018-4853 para esta vulnerabilidad.
- Ejecución de código arbitrario: Un atacante remoto con acceso al puerto 69/UDP podría modificar el cliente administrativo almacenado en el dispositivo. Si un usuario legítimo se descarga y ejecuta el cliente modificado, el atacante podría conseguir la ejecución de código en el sistema del cliente. Se ha reservado el identificador CVE-2018-4854 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han reservado los identificadores: CVE-2018-4855 y CVE-2018-4856.

Etiquetas: Siemens, Vulnerabilidad

Múltiples vulnerabilidades en Allen-Bradley Stratix 5950 de Rockwell Automation

Fecha de publicación: 04/07/2018

Importancia: Alta

Recursos afectados:

Los dispositivos Allen-Bradley Stratix 5950 usan el Adaptive Security Appliance (ASA), de Cisco Systems, como su sistema operativo central. Cisco ha publicado avisos que informan de múltiples vulnerabilidades en el software ASA. Los siguientes dispositivos Allen-Bradley Stratix 5950, que ejecutan Cisco ASA versión v9.6.2 y anteriores, se ven afectados:

- 1783-SAD4T0SBK9
- 1783-SAD4T0SPK9
- 1783-SAD2T2SBK9
- 1783-SAD2T2SPK9

Descripción:

Rockwell Automation ha identificado varias vulnerabilidades de validación impropia. Una explotación exitosa de estas vulnerabilidades podría permitir a un atacante evadir la certificación de cliente para crear conexiones al dispositivo afectado o provocar un bloqueo en el dispositivo.

Solución:

Rockwell Automation informarÃi a los usuarios de la actualización de firmware tan pronto como esté disponible. Mientras se publican, recomienda a los usuarios con productos afectados seguir las siguientes estrategias para mitigar los riesgos:

- CVE-2018-0228 ? Los comandos de configuración ASA y FTD pueden ser configurados para limitar el número de peticiones de conexión permitidas. El uso de estos parÃimetros de configuración puede reducir el número de conexiones y reducir en gran medida el impacto del ataque DoS.
- CVE-2018-0227 ? No hay soluciones disponibles.
- CVE-2018-0231 ? No hay soluciones disponibles.
- CVE-2018-0240 ? No hay soluciones disponibles.
- CVE-2018-0296 ? Cisco ha publicado una regla de snort que puede ser utilizada en IDS para protegerse. https://www.cisco.com/web/software/286271056/117258/sf-rules-2018-06-07-new.html

Detalle:

- Validación incorrecta de datos de entrada: Una vulnerabilidad en la funcionalidad de creación de flujo de ingreso de Cisco ASA podría permitir que un atacante remoto sin autenticar provoque un aumento en la utilización de la CPU al 100% dando lugar a una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2018-0228 para esta vulnerabilidad.
- Validación incorrecta de certificado: Una vulnerabilidad en la función de Autenticación del Certificado de Cliente de Cisco ASA podría permitir que un atacante remoto sin autenticar establezca una conexión SSL VPN y evada los pasos de verificación de certificado SSL. Se ha asignado el identificador CVE-2018-0227 para esta vulnerabilidad.
- Validación incorrecta de datos de entrada: Una vulnerabilidad en la librería de Securidad en la Capa de Transporte del software Cisco ASA y Cisco Firepower Threat Defense (FTD) podría permitir que un atacante remoto sin autenticar provoque una recarga en el dispositivo afectado dando lugar a una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2018-0231 para esta vulnerabilidad.
- Errores de administración de recursos: Múltiples vulnerabilidades en la función de inspección de protocolo de la capa de aplicación del software Cisco ASA y Cisco FTD podrían permitir que un atacante remoto sin autenticar provoque una recarga en el dispositivo afectado dando lugar a una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2018-0240 para esta vulnerabilidad.
- Validación incorrecta de datos de entrada: Una vulnerabilidad en la interfaz web de Cisco ASA podría permitir que un atacante remoto sin autenticar provoque una recarga en el dispositivo afectado dando lugar a una condición de denegación de servicio (DoS). También es posible en ciertas versiones de software que ASA no se recargue, y se podría obtener información sensible mediante salto de directorio. Se ha asignado el identificador CVE-2018-0296 para esta vulnerabilidad.

Etiquetas: Cisco, Vulnerabilidad

Validación incorrecta de los datos de entrada en Panel Builder 800 de ABB

Fecha de publicación: 09/07/2018

Importancia: Alta

Recursos afectados:

- Todas las versiones de Panel Builder 800

Descripción:

El investigador Michael DePlante de Leahy Center for Digital Investigation y Michael Flanders de Trend Micro, ambos trabajando con Zero Day Initiative de Trend Micro, han identificado una vulnerabilidad de validación incorrecta de los datos de entrada. Un potencial atacante podría aprovechar esta vulnerabilidad para insertar y ejecutar código arbitrario.

Solución:

ABB se encuentra actualmente investigando esta vulnerabilidad para proporcionar una protección adecuada a los usuarios. El problema será corregido en versiones futuras, no obstante, hasta que estén disponibles las actualizaciones de los productos afectados, se aconseja seguir las medidas de mitigación indicadas por el fabricante.
Las prácticas de seguridad recomendadas y las configuraciones de firewall pueden ayudar a proteger una red de control de procesos de los ataques que se originan fuera de la red.
Estas prácticas incluyen:

- Reforzar la concienciación sobre ciberseguridad para usuarios de Panel Builder 800:
  - Describiendo las recomendaciones generales de mejores prácticas de ciberseguridad para sistemas de control industrial.
  - Informando de que es posible infectar Panel Builder con malware.
  - Describiendo la importancia de ser cuidadoso con los ficheros que son recibidos inesperadamente y/o de fuentes desconocidas.
- Realizar una inspección cuidadosa de los archivos transferidos, incluyendo un escaneo de los mismos con un software antivirus actualizado, de manera que solo sean transferidos aquellos que sean legítimos.
- Gestionar de las cuentas de usuario, usando autenticación adecuada y la gestión de permisos utilizando el principio de mínimo privilegio.

Detalle:

Un atacante podría aprovechar la vulnerabilidad descrita en este aviso, engañando a un usuario para que abra un archivo especialmente diseñado. De esta manera, el atacante podría llegar a insertar o ejecutar código arbitrario. Hay que tener en cuenta que esta vulnerabilidad no se puede explotar de manera remota y no se puede aprovechar sin la interacción del usuario.

Etiquetas: Vulnerabilidad

Ejecución remota de código en productos Pepperl Fuchs

Fecha de publicación: 09/07/2018

Importancia: Alta

Recursos afectados:

- Todos los productos de las familias VisuNet RM, VisuNet PC y Box Thin Client BTC

Descripción:

Los investigadores de seguridad Eyal Karni, Yaron Zinar, Roman Blachman de Preempt y Research Labs han identificado una vulnerabilidad de ejecución remota de código en el protocolo Credential Security Support Provider (CredSSP) de Microsoft. Un potencial atacante podría aprovechar esta vulnerabilidad para retransmitir credenciales de usuario para la ejecución de código arbitrario en el sistema de destino.

Solución:

- Dispositivos Pepperl Fuchs HMI ejecutando RM Shell 4 deberían actualizar a RM Image 4 Security Patches 01/2017 a 05/2018 (18-33400C).
- Dispositivos Pepperl Fuchs HMI ejecutando RM Shell 5 deberían actualizar a RM Image 5 Security: Windows Cumulative Security Patch 07/2018 (18-33624).
- Dispositivos Pepperl Fuchs HMI ejecutando Windows 7 o Windows 10 deberían actualizar usando el mecanismo de actualización de Windows Update.
- Después de desplegar el parche, todos los clientes o servidores de terceros conectados deben usar la última versión del protocolo CredSSP.

Detalle:

Un potencial atacante podría ejecutar código arbitrario y obtener acceso a datos sensibles interceptando la conexión RDP inicial entre un cliente y un servidor remoto. Se require de un ataque MitM para controlar la sesión. Se ha reservado el identificador CVE-2018-0886 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Compass y AcSELerator Architect de Schweitzer Engineering Laboratories, Inc.

Fecha de publicación: 11/07/2018

Importancia: Alta

Recursos afectados:

- Compass, versión 3.0.5.1 y anteriores
- AcSELerator Architect, versión 2.2.24.0 y anteriores (ICD package versión 2.38.0)

Descripción:

El investigador Gjoko Krstic de Applied Risk ha identificado varias vulnerabilidades de tipo permisos inadecuados, restricción inadecuada en referencias a entidades y consumo de recursos no controladas en los productos Compass y AcSELerator Architect de Schweitzer Engineering Laboratories (SEL que podrían provocar la escalada de privilegios o denegaciones de servicio.

Solución:

- Para SEL Compass v3.0.6.1 o posterior, aplicar la actualización disponible en https://selinc.com/products/compass/#tab-downloads
- Para SEL AcSELerator v2.2.29.0 (ICD 2.44.0) o posterior, aplicar la actualización disponible en https://selinc.com/products/5032/#tab-downloads

Detalle:

- Permisos por defecto incorrectos podrían permitir a un atacante el acceso completo a los directorios de Compass, la modificación o sobreescritura de ficheros en el directorio de instalación de Compass, obteniendo una escalada de privilegios y la ejecución de código malicioso. Se ha reservado el identificador CVE-2018-10604 para esta vulnerabilidad.
- Restricciones inadecuadas a referencias a entidades XML externas (XXE) podrían permitir a unatacante aprovechar las entradas no verificadas facilitadas al parseador XML de AcSELerator Architect para conseguir la divulgación de datos arbitrarios, la ejecución de código arbitrario o denegaciones de servicio. Se ha reservado el identificador CVE-2018-10600 para esta vulnerabilidad.
- Un consumo de recursos no controlado podría permitir a un atacante la utilización del cliente FTP de AcSELerator Architect para conectarse a un servidor malicioso, lo que podría causar un consumo del 100% de uso de CPU y llevar a una condición de denegación de servicio. El reinicio de la aplicación es requerido para restablecer el servicio. Se ha reservado el identificador CVE-2018-10608 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Robot Controllers de Universal Robots

Fecha de publicación: 11/07/2018

Importancia: Crítica

Recursos afectados:

- CB 3.1, SW versión 3.4.5-100

Descripción:

Varios investigadores del Politecnico di Milano trabajando con Forward-Looking Threat Research Team de Trend Micro, han reportado varias vulnerabilidades de tipo contraseñas embebidas y falta de autenticación en el producto Robot Controllers de Universal Robots. Un potencial atacante remoto podría llegar a ejecutar código arbitrario en el dispositivo.

Notar que Cesar Cerrudo y Lucas Apa en su presentación Hacking Robots Before Skynet ya informaron de la vulnerabilidad con el identificador CVE-2018-10635.

Solución:

Universal Robots recomienda las siguientes acciones preventivas:

- Permitir el acceso físico a la caja de control del robot y al terminal de programación solo a usuarios de confianza.
- No conectar el robot a una red a no ser que sea requerido por la aplicación.
- No conectar el robot directamente a Internet. Usar una red segura con una configuración correcta del cortafuegos (los puertos TCP 30001 y 30003 deben estar restringidos).
- Crear una subred privada donde la interfaz de red del robot esté expuesta lo menos posible.

Detalle:

- Uso de contraseñas embebidas. La aplicación utiliza credenciales embebidas que podrían permitir a un atacante restablecer las contraseñas del controlador. Se ha asignado el identificador CVE-2018-10633 para esta vulnerabilidad.
- Falta de autenticación en función crítica. Los puertos TCP 30001 y 30003 escuchan código URScript arbitrario y lo ejecutan. Esto permitiría a un atacante remoto con acceso a los puertos la ejecución de código. Se ha asignado el identificador CVE-2018-10635 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en e!DISPLAY de WAGO

Fecha de publicación: 11/07/2018

Importancia: Alta

Recursos afectados:

- WAGO e!DISPLAY 762-3000
- WAGO e!DISPLAY 762-3001
- WAGO e!DISPLAY 762-3002
- WAGO e!DISPLAY 762-3003

Descripción:

El investigador T. Weber de SEC-Consult ha identificado múltiples vulnerabilidades de los tipos XSS, validación incorrecta de parámetros de entrada y gestión incorrecta de permisos. Un atacante podría aprovechar estas vulnerabilidades para ejecutar código arbitrario en el contexto del usuario, reemplazar ficheros existentes o inyectar código persistente.

Solución:

WAGO recomienda actualizar a la última versión del firmware (FW02). En caso de no ser posible la actualización, el fabricante aconseja limitar los accesos a usuarios y dispositivos confiables.

Para más detalle sobre cómo obtener el nuevo firmware, deberá ponerse en contacto con el equipo de soporte del fabricante

Detalle:

- Una vulnerabilidad debida a una incorrecta neutralización de entradas durante la generación de la página Web (XSS), podría permitir a un atacante, con o sin autenticación, enviar peticiones especialmente diseñadas para inyectar código en el WBM. Este código malicioso sería renderizado o ejecutado en el navegador del usuario final. Se ha reservado el identificador CVE-2018-12981 para esta vulnerabilidad.
- Una vulnerabilidad debida a una restricción inadecuada en la carga de tipos de ficheros peligrosos, podría permitir a un atacante autenticado, subir ficheros arbitrarios en el sistema de archivos con los permisos del servidor web. Se ha reservado el identificador CVE-2018-12980 para esta vulnerabilidad.
- Una vulnerabilidad debida a una incorrecta asignación de permisos para los recursos críticos, podría permitir a un atacante sobrescribir ficheros críticos del sistema, aprovechándose de la vulnerabilidad anteriormente descrita. Se ha reservado el identificador CVE-2018-12979 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Denegación de servicio en módulos de comunicación Ethernet EN100 y relés SIPROTEC 5 de Siemens

Fecha de publicación: 12/07/2018

Importancia: Alta

Recursos afectados:

- Variantes de firmware IEC 61850 para EN100 Ethernet Module, todas las versiones anteriores a la V4.33
- Variantes de firmware PROFINET IO, Modbus TCP, DNP3 TCP e IEC104 para EN100 Ethernet Module, todas las versiones.
- Relés SIPROTEC 5 con las variantes de CPU CP300 y CP100 y los respectivos módulos de comunicación Ethernet, todas las versiones anteriores a V7.80 (solo afectados por CVE-2018-11451).
- Relés SIPROTEC 5 con las variantes de CPU CP200 y los respectivos módulos de comunicación Ethernet, todas las versiones (solo afectados por CVE-2018-11451).

Descripción:

Victor Nikitin, Vladislav Suchkov y Ilya Karpov de ScadaX han identificado varias vulnerabilidaes de tipo denegación de servicio que afectan a módulos de comunicación Ethernet EN100 y relés SIPROTEC 5 de Siemens. Un posible atacante podría aprovechar estas vulnerabilidades para causar una denegación de servicio en los productos afectados.

Solución:

- Variante de firmware IEC 61850 de EN100: Actualizar a la versión V4.33 disponible en https://support.industry.siemens.com/cs/us/en/view/109745821
- Variantes de firmware PROFINET IO, Modbus TCP, DNP3 TCP e IEC104 de EN100 y SIPROTEC 5 con las variantes de CPU CP200 y los respectivos módulos de comunicación Ethernet: Bloquear el acceso al puerto TCP 102, por ejemplo, con un cortafuegos externo.
- SIPROTEC 5 con las variantes de CPU CP300 y CP100 y los respectivos módulos de comunicación Ethernet: Actualizar a la versión de firmware V7.80 para los siguientes tipos de dispositivos. 6MD85, 6MD86, 7SS85, 7KE85,7UM85, 7SA87, 7SD87, 7SL87, 7VK87, 7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86, 7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82, 7UT85, 7UT86, y 7UT87.

Detalle:

- Un atacante con acceso de red podría enviar un paquete específicamente diseñado al puerto TCP 102 y causar una condición de denegación de servicio en los productos afectados. Un reinicio manual es necesario para restablecer la funcionalidad del módulo EN100 en SIPROTEC 4 y los relés SIPROTEC Compact. Como condición previa, la comunicación IEC 61850-MMS debe activarse en los productos o módulos afectados. Se ha asignado el identificador CVE-2018-11451 para esta vulnerabilidad.
- Un atacante con acceso de red podría enviar un paquete específicamente diseñado al puerto TCP 102 y causar una condición de denegación de servicio en el módulo de comunicación EN100 si los osciló grafos se están ejecutando. Un reinicio manual es necesario para restablecer la funcionalidad del módulo EN100. Como condición previa, la comunicación IEC 61850-MMS debe activarse en los módulos EN100 afectados. Esta vulnerabilidad no afecta a los relés SIPROTEC 5. Se ha asignado el identificador CVE-2018-11452 para esta vulnerabilidad.

Etiquetas: Siemens, Vulnerabilidad

Desbordamiento de búfer en 9000X Drive de Eaton

Fecha de publicación: 13/07/2018

Importancia: Media

Recursos afectados:

- 9000X Drive, versión 2.0.29 y anteriores

Descripción:

El investigador Ghirmay Desta, trabajando con Zero Day Initiative de Trend Micro, ha identificado una vulnerabilidad de desbordamiento de búfer en 9000X Drive de Eaton. Un potencial atacante podría llegar a ejecutar código remoto en los productos afectados.

Solución:

Eaton ha publicado la versión v2.0.28 para 9000X Drive que soluciona esta vulnerabilidad. Puede descargarse en el siguiente enlace: http://www.eaton.com/Eaton/ProductsServices/Electrical/ProductsandServices/AutomationandControl/AdjustableFrequencyDrives/IndustrialDrives/SVX/index.htm#tabs-4

Detalle:

Una vulnerabilidad de desbordamiento de búfer presente en los productos afectados, podría permitir a un potencial atacante la ejecución de código remoto. Se ha asignado el identificador CVE-2018-8847 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Consumo de recursos no controlado en Nport 5210, 5230 y 5232 de Moxa

Fecha de publicación: 20/07/2018

Importancia: Alta

Recursos afectados:

Nport 5210, 5230 y 5232 Versiones 2.9 build 17030709 y anteriores.

Descripción:

Mikael Vingaard ha reportado esta vulnerabilidad a NCCIC/ICS-CERT. Un atacante podría aprovechar esta vulnerabilidad enviando paquetes TCP SYN, con el fin de

consumir todos los recursos, dejando al dispositivo no disponible.

Solución:

Moxa recomienda a los usuarios que actualicen a la última versión de firmware, la cual se encuentra disponible en:

https://www.moxa.com/support/download.aspx?type=support&id=904

Detalle:

La cantidad de recursos solicitados por un posible atacante no está restringida, lo que permite explotar esta vulnerabilidad para consumir los recursos disponibles, provocando una condición de denegación de servicio. Se ha asignado el identificador CVE-2018-10632 para esta vulnerabilidad

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en SmartServer 1, SmartServer 2, i.LON 100 e i.LON 600 de Echelon.

Fecha de publicación: 20/07/2018

Importancia: Crítica

Recursos afectados:

- SmartServer 1, i.LON 100 e i.LON 600, todas las versiones
- SmartServer 2 todas las versiones anteriores a 4.11.007

Descripción:

Echelon, junto con Daniel Crowley, e IBM?s X-Force Red Team han reportado estas vulnerabilidades a NCCIC/ICS-CERT. Una explotación exitosa de estas vulnerabilidades podría permitir la ejecución remota de código en el dispositivo.

Solución:

Echelon recomienda a los usuarios afectados instalar SmartServer 2 Service Pack 7 (Version 4.11.007) para mitigar CVE-2018-8859, CVE-208-8851 y CVE-2018-8855, el cual se puede descargar en el siguiente enlace:

https://www.echelon.com/software-downloads?ele=153-0608-01A

También se recomienda la siguiente mitigación manual:

Para el CVE-2018-10627 Echelon recomienda a los usuarios afectados modificar el fichero WebParams.dat.

Echelon recomienda que se implemente la siguiente mitigación hasta que se instale SmartServer 2 Service Pack 7:

- Todos los dispositivos SmartServer e i.LON 600 junto con los servidores que utilizan los servicios SmartServer e i.Lon deben instalarse detrás de un cortafuegos o en una VLAN sin otros dispositivos.
- Cambie el nombre de usuario y la contraseña durante la instalación inicial de los productos afectados
- Deshabilite servicios no cifrados y servicios cifrados seguros para SmartServer o i.LON 100

Detalle:

- **Exposición de información**: Un atacante puede usar el API SOAP para recuperar y modificar elementos de configuración sensibles, como los nombres de usuario y contraseñas de los servidores web y FTP. Esta vulnerabilidad no afecta al producto i.LON 600. Se ha asignado el identificador CVE-2018-10627 para esta vulnerabilidad.
- **Evasión de la autenticación utilizando un camino o canal alternativo**: Un atacante puede eludir la autenticación requerida especificada en el archivo de configuración de seguridad al incluir caracteres adicionales en el nombre de directorio cuando se especifica el directorio al que se accederá. Esta vulnerabilidad no afecta al producto i.LON 600. Se ha asignado el identificador CVE-2018-8859 para esta vulnerabilidad.
- **Almacenamiento de credenciales sin protección**: Los dispositivos almacenan contraseñas en texto plano, lo que podría permitir a un atacante con acceso al archivo de configuración inicie sesión en la interfaz de usuario web de SmartServer. Se ha asignado el identificador CVE-2018-8851 para esta vulnerabilidad.
- **Transmisión de información sensible en texto claro**: Los dispositivos permiten conexiones web sin cifrado por defecto y los dispositivos pueden recibir actualizaciones de configuración y de firmware mediante FTP inseguro. Se ha asignado el identificador CVE-2018-8855 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en software InduSoft e InTouch de AVEVA

Fecha de publicación: 20/07/2018

Importancia: Crítica

Recursos afectados:

- InduSoft Web Studio v8.1 y v8.1 SP1.
- InTouch Machine Edition v2017 8.1 y v2017 8.1 SP1.
- InTouch 2014 R2 SP1 y anteriores.
- InTouch 2017.
- InTouch 2017 Update 1.
- InTouch 2017 Update 2.

Descripción:

George Lashenko de CyberX e investigadores de Tenable Research han identificado vulnerabilidades de tipo desbordamiento de búfer, relacionadas con el software InduSoft e InTouch de AVEVA, lo que permitiría a un atacante remoto la ejecución de código.

Solución:

Los usuarios de InduSoft Web Studio v8.1 SP1 deberán aplicar lo antes posible el parche InduSoft Web Studio Hotfix 81.1.00.08. Los usuarios de InduSoft Web Studio v8.1 deberán actualizar a la versión SP1, y posteriormente aplicar el parche.

Los usuarios de InTouch Machine Edition 2017 v8.1 SP1 deberán aplicar lo antes posible el parche InTouch Machine Edition Hotfix 81.1.00.08. Los usuarios de InTouch Machine Edition 2017 v8.1 deberán actualizar a la versión SP1, y posteriormente aplicar el parche.

http://www.indusoft.com/File-Management?Command=Core_Download&EntryId=2074

https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=5063

Para el software InTouch 2014 R2 SP1, aplicar el parche HF-11_1_SP1/CR149705 lo antes posible, los usuarios de versiones anteriores deberán primero actualizar a una versión con parche y aplicarlo.

https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=5057

El parche para InTouch 2017 Update 2 es HF-17_2/CR149706, las versiones anteriores deben previamente actualizarse Update 2, y posteriormente parchear.

https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=5058

Para ver más detalle ver los enlaces de referencia.

Detalle:

- **Desbordamiento de búfer en InduSoft Web Studio e InTouch Machine Edition**: Un potencial atacante remoto, podría enviar peticiones especialmente diseñadas para explotar esta vulnerabilidad de desbordamiento de búfer, durante acciones de petición de lectura o escritura sobre ciertas etiquetas, alarmas o eventos, lo que le permitiría la ejecución remota de código. Se ha asignado el identificador CVE-2018-10620 para esta vulnerabilidad.
- **Desbordamiento de búfer en InTouch**: Un potencial atacante sin autenticación en el sistema podría enviar un paquete especialmente diseñado para causar un desbordamiento de búfer por una gestión incorrecta de enteros en punto flotante. Esta vulnerabilidad permitiría la ejecución de código con los mismos privilegios que el proceso de InTouch View. Se ha asignado el identificador CVE-2018-10628 para esta vulnerabilidad.

Etiquetas: 0day, Vulnerabilidad

Múltiples vulnerabilidades en MicroSCADA Pro SYS600

Fecha de publicación: 23/07/2018

Importancia: Crítica

Recursos afectados:

MicroSCADA Pro SYS600 9.2, 9.3, 9.4

Descripción:

El investigador Vladimir Dashchenko de Kaspersky Labs ha reportado esta vulnerabilidad en las versiones del producto indicado anteriormente. Un atacante autenticado podría explotar esta vulnerabilidad lo cual provocaría un bloqueo remoto del proceso o la ejecución de código arbitrario en el sistema afectado.

Además, Microsoft ha documentado un problema conocido (bucle de reinicio), con los controladores antiguos Sentinel HASP, al implementar actualizaciones de seguridad de Microsoft en marzo de 2018 y siguientes. ABB ha confirmado los problemas de reinicio de bucle con al menos los sistemas Windows 7 y Windows Server 2008 SP2. Se recomienda seguir las instrucciones de este aviso para instalar la versión Sentinel HASP / LDK 7.80 con los controladores más recientes antes de implementar las actualizaciones de seguridad de Microsoft.

Solución:

El problema se soluciona por Gemalto en la siguiente versión del producto:

- Versión 7.80 de Sentinel HASP/LDK License Manager

ABB recomienda a los usuarios afectados aplicar esta actualización lo antes posible.

La actualización es soportada en los siguientes sistemas operativos: Windows 7 SP1, Windows 8.1 SP1, Windows Server 2008 R2 SP1, Windows Server 2012 R2, Windows Server 2016, Windows 10 Version 1709. Antiguas versiones del sistema operativo probablemente son también completamente compatibles, pero Gemalto no lo garantiza. Fuera de los sistemas operativos mencionados anteriormente, ABB ha probado la actualización en Windows Server 2008 SP2.

Detalle:

Ejecución remota de código arbitrario: Un atacante podría explotar la vulnerabilidad existente en el servicio Sentinel HASP Run?time Environment de forma remota, subiendo un fichero especialmente creado al mismo provocando un desbordamiento de búfer que permitiría ejecutar código arbitrario o apagar el proceso remoto (una denegación de servicio). Se han asignado los identificadores CVE-2017-11498, CVE-2017-11497, CVE-2017-11496, CVE-2017-12818, CVE-2017-12819, CVE-2017-12820, CVE-2017-12821, CVE-2017-12822 para esta vulnerabilidad.

Etiquetas: SCADA, Vulnerabilidad

Múltiples desbordamientos de búfer en LeviStudioU de Wecon

Fecha de publicación: 27/07/2018

Importancia: Crítica

Recursos afectados:

LeviStudioU

Descripción:

El equipo de seguridad de nfocus y el investigador Mat Powell de Zero Day Initiative de Trend Micro han reportado una serie de vulnerabilidades de tipo desbordamiento de búfer que afectan al software LeviStudioU del fabricante Wecon. Estas vulnerabilidades permitirían a un potencial atacante ejecutar código remoto bajo permisos de administrador.

Solución:

Actualmente no existe mitigación o algún tipo de solución para estas vulnerabilidades.

Se recomienda aislar los dispositivos que utilicen el software afectado y controlar los accesos que se tienen a los mismos.

Además, para proteger los recursos afectados se recomienda:

- Ayudar a minimizar la exposición de todos los dispositivos y/o sistemas de control tras cortafuegos y confirmar que los dispositivos y/o sistemas no poseen acceso a Internet.
- Separar las redes de control y los dispositivos industriales de las redes corporativas.
- Cuando sea necesario un acceso remoto, utilizar mecanismos de seguridad como Virtual Private Networks (VPN).

Detalle:

Algunos ficheros, como los UMP, HSC o los HGCM, no realizan un correcto tratamiento de la longitud en diferentes campos que contienen. Este hecho origina un desbordamiento de búfer. Otros ficheros más concretos, como UserMgr.xml, TTS.xml o ejecutables como UserManage.exe, etc., también tienen problemas a la hora de gestionar tanto parámetros como otros elementos que contienen.

Zero Day Initiative ha asignado los identificadores que van desde el ZDI-18-784 al ZDI-18-873 para estas vulnerabilidades críticas.

Etiquetas: 0day, Vulnerabilidad

Múltiples vulnerabilidades en funcionalidades TCPdump en productos Hirschmann

Fecha de publicación: 30/07/2018

Importancia: Alta

Recursos afectados:

- HiOS, versión 07.0.00 y anteriores de los siguientes productos:
  - RSP
  - RSPE
  - RSPS
  - RSPL
  - MSP
  - EES
  - EESX
  - GRS
  - OS
  - RED
- Classic, todas las versiones de los siguientes productos:
  - RS
  - RSR
  - RSB
  - MACH100
  - MACH1000
  - MACH4000
  - MS
  - OCTOPUS
- Cellular Router, versión 01.2.02 y anteriores del siguiente producto:
  - OWL

Descripción:

Belden ha comunicado múltiples vulnerabilidades en funcionalidades TCPdump en diferentes familias de productos y plataformas de Hirschmann. Estas vulnerabilidades de desbordamiento de búfer podrían permitir a un potencial atacante remoto originar denegaciones de servicio o realizar ejecuciones de código remoto.

Solución:

El fabricante recomienda a sus clientes actualizar los productos lo antes posible siempre y cuando sea posible.

- HiOS: Actualizar todos los productos a la versión 07.0.01.
- Classic: No se tiene planeada ninguna actualización para estos productos.
- Cellular Router:
  - OWL LTE M12: Actualizar a la versión 01.2.03
  - OWL LTE, OWL 3G: Solución planificada para la versión 02.0.00.

Detalle:

El incorrecto tratamiento de los parámetros de entrada que realizan las funciones incluidas dentro de TCPdump (versiones anteriores a la 4.9.2), permitiría a un atacante remoto originar denegaciones de servicio o realizar ejecuciones de código.

Las vulnerabilidades sólo pueden ser explotadas durante una sesión activa que utilice las funciones TCPdump y el tráfico de red esté gestionado directamente por el producto afectado. La funcionalidad TCPdump está inactiva por defecto.

Se han asignado los siguientes identificadores para estas vulnerabilidades: CVE-2017-12894, CVE-2017-12996, CVE-2017-12988, CVE-2017-13012, CVE-2017-13013, CVE-2017-13022, CVE-2017-13030, CVE-2017-13037, CVE-2016-7923, CVE-2016-7926, CVE-2016-7932, CVE-2016-7936, CVE-2016-7974, CVE-2016-7975, CVE-2016-7983, CVE-2016-7984.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad