Boletín de noviembre de 2018

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en CirCarLife de Circontrol

Fecha de publicación: 02/11/2018

Importancia: Crítica

Recursos afectados:

- CirCarLife todas las versiones anteriores a 4.3.1

Descripción:

Ankit Anubhav de NewSky Security, M. Can Kurnaz de KMPG Holanda, Alim Solmaz de Atos, Michael Jonh de WePower Network y Gyorgy Miru de Verint han reportado estas vulnerabilidades de tipo evasión de autenticación y credenciales insuficientemente protegidas. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto obtener credenciales almacenadas en texto plano, evadir la autenticación así como ver y acceder a información crítica.

Solución:

Circontrol ha publicado una nueva versión de software que soluciona estas vulnerabilidades, disponible en el siguiente enlace:

http://expertarea.circontrol.com/

Detalle:

- **Evasión de autenticación:** La autenticación en el dispositivo puede ser evitada introduciendo una URL de un sitio específico. Se ha reservado el identificador CVE-2018-17928 para esta vulnerabilidad.
- **Credenciales insuficientemente protegidas:** Las credenciales PAP del dispositivo son almacenadas en texto plano dentro de un fichero de *log* que es accesible sin autenticación. Se ha reservado el identificador CVE-2018-17922 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Restricción indebida de referencias XXE en CASE Suite de Fr. Sauter AG

Fecha de publicación: 02/11/2018

Importancia: Alta

Recursos afectados:

- CASE Suite versión 3.10 y anteriores

Descripción:

El investigador Gjoko Krstic de Applied Risk ha identificado una vulnerabilidad del tipo restricción indebida de referencias XXE (XML External Entity) que podría permitir a un atacante remoto conseguir archivos sin autorización.

Solución:

Fr. Sauter AG aconseja utilizar Service Release 1 para los dispositivos que tengan CASE Suite versión 3.10 o anteriores. El software se encuentra disponible mediante los canales locales de soporte.

Detalle:

Existe una vulnerabilidad de restricción incorrecta de referencias XXE (XML External Entity) a la hora de procesar los parámetros de identidades XML que podría permitir la divulgación de ficheros de manera remota. Se ha asignado el identificador CVE-2018-17912 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en InduSoft Web Studio e InTouch Edge HMI de AVEVA

Fecha de publicación: 02/11/2018

Importancia: Crítica

Recursos afectados:

- InduSoft Web Studio todas las versiones anteriores a 8.1 SP2
- InTouch Edge HMI (antes InTouch Machine Edition) todas las versiones anteriores a 2017 SP2

Descripción:

Tenable ha reportado estas vulnerabilidades de tipo desbordamiento de búfer y ausencia de contraseña en fichero de configuración. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante la ejecución remota de código.

Solución:

AVEVA recomienda a los usuarios afectados actualizar InduSoft Web Studio a la versión 8.1 SP2 y InTouch Edge HMi a la versión 2017 SP2. Dichas actualizaciones pueden ser descargadas desde el Global Customer Support en el área Software Download o a través de los siguientes enlaces:

- InduSoft Web Studio
- InTouch Edge HMI

Detalle:

- Desbordamiento de búfer: un atacante remoto podría enviar un paquete especialmente diseñado que podría provocar un desbordamiento de búfer durante las acciones relacionadas con etiquetas, alarmas o eventos, como lecturas y escrituras, pudiendo llegar a ejecutarse código. Si no se ha habilitado la seguridad de comunicaciones remotas en InduSoft Web Studio o no se utiliza contraseña, un atacante podría enviar un paquete especialmente diseñado para invocar un proceso arbitrario, pudiendo llegar también a ejecutarse código. El código, que se ejecutaría bajo los privilegios del proceso en ejecución de InduSoft Web Studio o InTouch Edge HMI podría comprometer ambos equipos. Se ha asignado el identificador CVE-2018-17916 para esta vulnerabilidad.
- Ausencia de contraseña en fichero de configuración: esta vulnerabilidad podría permitir a un atacante remoto sin autenticación la ejecución de código de manera remota con los mismos privilegios que el proceso en ejecución de InduSoft Web Studio o InTouch Edge HMI. Se ha asignado el identificador CVE-2018-17914 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en dispositivos médicos portátiles Point of Care de Roche

Fecha de publicación: 07/11/2018

Importancia: Alta

Recursos afectados:

- Accu-Chek Inform II.
- CoaguChek Pro II, XS Plus y XS Pro.
- cobas h 232 POC.
- Se incluyen las unidades de base (BU), los núcleos de la unidad de base y las unidades de base portátiles (HBU) relacionadas con los equipos.

Descripción:

El investigador Niv Yehezkel de Medigate ha identificado varias vulnerabilidades de tipo autenticación inadecuada, inyección de comandos en el sistema operativo, carga de ficheros potencialmente peligrosos sin restricción y control de acceso inadecuado que afectan a diferentes dispositivos médicos portátiles Point of Care de Roche. Un potencial atacante podría conseguir acceso no autorizado para modificar la configuración del sistema o la ejecución de código arbitrario.

Solución:

Roche recomienda aplicar las siguientes medidas:

- Dispositivos conectados (Ethernet y Wifi):
  - Restringir el acceso físico y de red al dispositivo y a la infraestructura conectada, habilitando las funciones de seguridad del dispositivo.
  - Proteger los dispositivos finales conectados de accesos no autorizados, robo y software malintencionado.
  - Monitorizar el sistema y la infraestructura de red en busca de actividades sospechosas e informar de un posible compromiso según la política local.
- Dispositivos no conectados:
  - Proteger contra el acceso no autorizado, el robo y la manipulación.

Detalle:

- Un potencial atacante en una red adyacente podría aprovechar credenciales de acceso débiles para conseguir un acceso no autorizado mediante la interfaz de servicio. Se ha reservado el identificador CVE-2018-18561 para esta vulnerabilidad.

- Los permisos inseguros en una interfaz de servicio pueden permitir que los atacantes autenticados en la red adyacente, ejecuten comandos arbitrarios en los sistemas operativos. Se ha reservado el identificador CVE-2018-18562 para esta vulnerabilidad.
- Una vulnerabilidad en el mecanismo de actualización del software permite a un atacante en una red adyacente sobrescribir archivos arbitrarios en el sistema a través de un paquete de actualización manipulado. Se ha reservado el identificador CVE-2018-18563 para esta vulnerabilidad.
- Un potencial atacante en una red adyacente podría ejecutar código arbitrario en el sistema mediante paquetes manipulados o cambiar la configuración del instrumento gracias a un control de acceso inadecuado. Se han reservado los identificadores CVE-2018-18564 y CVE-2018-18565 para estas vulnerabilidades.

Etiquetas: Vulnerabilidad

Denegación de servicio en controladores MicroLogix 1400 y módulos de comunicación EtherNet/IP 1756 ControlLogix de Rockwell Automation

Fecha de publicación: 08/11/2018

Importancia: Alta

Recursos afectados:

- Controladores MicroLogix 1400:
  - Series A, todas las versiones
  - Series B y C, versión 21.003 y anteriores
- Módulos de comunicación EtherNet/IP 1756 ControlLogix:
  - 1756-ENBT, todas las versiones
  - 1756-EWEB, Series A y B, todas las versiones
  - 1756-EN2F
    - Series A y B, todas las versiones
    - Series C, versión 10.10 y anteriores
  - 1756-EN2T
    - Series A, B y C, todas las versiones
    - Series D, versión 10.10 y anteriores
  - 1756-EN3TR
    - Series A y B, todas las versiones
    - Series C, versión 10.10 y anteriores

Descripción:

ICS-CERT ha reportado a Rockwell Automation una vulnerabilidad de tipo denegación de servicio que afecta a los dispositivos controladores MicroLogix 1400 y a los módulos de comunicación EtherNet/IP 1756 ControlLogix de Rockwell Automation. Un atacante remoto sin autenticar podría interrumpir la comunicación Ethernet mediante cambios en la configuración IP del dispositivo afectado.

Solución:

Para los dispositivos Controladores MicroLogix 1400 Series B o C, Rockwell Automation recomienda:

- Actualizar a la versión FRN 21.004
- Una vez aplicada la actualización, poner el dispositivo en modo RUN para prevenir cambios en el dispositivo

Para los módulos de comunicación EtherNet/IP 1756 ControlLogix 1756-EN2F Series C, 1756-EN2T Series D, 1756-EN2TR Series C y 1756-EN3TR Series B Rockwell Automation recomienda:

- Actualizar a la versión FRN 11.001
- Una vez aplicada la actualización habilitar *Explicit Protected Mode*.

Para el resto de los dispositivos no existe parche o actualización que solucione esta vulnerabilidad y el fabricante recomienda seguir sus directrices generales de seguridad.

Detalle:

- Un atacante remoto sin autenticación podría causar la denegación del servicio mediante el envío de una petición de conexión CIP y, una vez conectado, enviar una nueva configuración IP al dispositivo afectado, incluso si el controlador del sistema está configurado en modo Hard RUN. Cuando el dispositivo afectado acepta esta nueva configuración pierde todas las comunicaciones con el resto del sistema, esto se debe a que el tráfico del sistema sigue intentando comunicarse con la antigua dirección IP, la cual ha sido sobrescrita.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Requisitos insuficientes en la autenticación en iSite y IntelliSpace PACS de Philips

Fecha de publicación: 09/11/2018

Importancia: Media

Recursos afectados:

- iSite PACS, todas las versiones.
- IntelliSpace PACS, todas las versiones.

Descripción:

Un usuario ha reportado una vulnerabilidad relacionada con la falta de requisitos lo suficientemente robustos con respecto a las contraseñas en equipos de Philips. Posteriormente a este reporte, Philips ha informado al NCCIC. La explotación exitosa de esta vulnerabilidad, puede permitir a un potencial atacante con acceso a la red local donde se encuentra el dispositivo vulnerable, comprometer componentes del sistema.

Solución:

Philips recomienda a sus clientes que las instalaciones de su producto IntelliSpace PACS se realicen en un entorno controlado siguiendo las recomendaciones proporcionadas por el NCCIC a la hora de minimizar los riesgos de explotación (uso de VPN, cortafuegos para aislar las redes entre sí, evitar que los dispositivos vulnerables tengan acceso a Internet, etc.).

Adicionalmente, Philips proporciona a sus clientes una solución de antivirus automatizada que monitoriza y corrige continuamente las amenazas en todos los entornos que poseen servicios gestionados. Por otro lado, Philips también posee un programa de parches mensual proporcionado a todos los usuarios de IntelliSpace PACS que deseen participar en dicho programa.

La plataforma Philips iSite 3.6, se encuentra actualmente en su final de vida útil (*End of Life*, EoL) y en su final de servicio (*End of Service*, EoS).

Como mitigación provisional de la vulnerabilidad, Philips recomienda a los usuarios:

- Asegurarse de que solo el personal autorizado puede conectarse a los entornos donde se encuentran productos afectados por la vulnerabilidad.
- Revisar las instrucciones de uso disponibles con respecto a la interfaz de aplicación y seguir las guías de buenas prácticas en materia de ciberseguridad.

Para más información, Philips proporciona los siguientes contactos:

- Ayuda y soporte técnico sobre la vulnerabilidad
- Consultas sobre la ciberseguridad de equipos Philips

Detalle:

- Las credenciales por defecto y la ausencia de mecanismos de autenticación dentro del software de terceros, podrían permitir a un potencial atacante con acceso a la red local, comprometer componentes del sistema donde se encuentra el producto afectado. La explotación exitosa de esta vulnerabilidad tiene un impacto directo en la confidencialidad, integridad y disponibilidad de los componentes comprometidos del sistema.

Etiquetas: Privacidad, Vulnerabilidad

Múltiples vulnerabilidades en productos Siemens

Fecha de publicación: 13/11/2018

Importancia: Alta

Recursos afectados:

- Las CPU S7-400 (CVE-2018-16556 y CVE-2018-16557):
  - SIMATIC S7-400 V6 (incl. F) e inferiores, todas las versiones.
  - SIMATIC S7-400 PN/DP V7 (incl. F), todas las versiones.
  - SIMATIC S7-400H V4.5 e inferiores, todas las versiones.
  - SIMATIC S7-410, todas las versiones anteriores a 8.2.1
- Paneles SIMATIC HMI 4" - 22", Paneles SIMATIC HMI Comfort Outdoor 7" y 15", Paneles móviles SIMATIC HMI KTP KTP400F, KTP700, KTP700F, KTP900 y KTP900F, SIMATIC WinCC Runtime Advanced, SIMATIC WinCC Runtime Professional, SIMATIC WinCC Runtime Professional y SIMATIC WinCC Runtime Professional, todas las versiones anteriores a 15 Update 4. (CVE-2018-13814, CVE-2018-13812 y CVE-2018-13813)
- SCALANCE S602, SCALANCE S612, SCALANCE S623 y SCALANCE S627-2M versiones anteriores a 4.0.1.1 (CVE-2018-16555)
- SIMATICS S7-1200, todas las versiones (CVE-2018-13815)
- SIMATICS S7-1500, todas las versiones anteriores a 2.6 (CVE-2018-13815)
- SIMATIC STEP 7, todas las versiones anteriores a 15.1 (CVE-2018-13811)
- SIMATIC IT LMS, todas las versiones (CVE-2018-13804)
- SIMATIC IT Production Suite, todas las versiones anteriores a la 7.1 Upd3 (CVE-2018-13804)
- SIMATIC IT UA Discrete Manufacturing, todas las versiones anteriores a la 1.2 y 1.3, 2.3, 2.4 (CVE-2018-13804)

Descripción:

Siemens ha publicado múltiples vulnerabilidades de tipo inyección de cabeceras HTTP, redirecciones a URLs no controladas, XSS, incorrecta gestión de paquetes, evasión de autenticación y almacenamiento de contraseñas en texto plano. Éstas podrían permitir a un atacante con acceso a los dispositivos o a la red donde se encuentran los recursos afectados originar denegaciones de servicio, obtener información sensible, realizar ejecuciones en el lado del cliente vía web y engañar a los usuarios registrados en las plataformas afectadas para posteriormente ejecutar acciones maliciosas.

Siemens agradece a los siguientes CERT e investigadores la coordinación de estas vulnerabilidades:

- CNCERT/CC (CVE-2018-16556)
- Hosni Tounsi de Carthage Red Team (CVE-2018-13812)
- Nelson Berg de Applied Risk (CVE-2018-16555)
- Younes Dragoni de Nozomi Networks y el ICS-CERT (CVE-2018-13813)

Las demás vulnerabilidades han sido gestionadas por el propio equipo de seguridad de Siemens.

Solución:

Siemens recomienda las siguientes acciones para mitigar las vulnerabilidades:

- CVE-2018-16557:
  - Configurar la protección de nivel 3 (protección de lectura/escritura)
- CVE-2018-16556:
  - Para las CPU SIMATIC S7-CPU 410, activar la seguridad de la interfaz de campo en PCS 7 V9.0 y utilizar un SIMATIC CP443-1 Adv. para comunicarse con ES/OS.

    - Aplicar el concepto de defensa en profundidad publicado por Siemens .
- CVE-2018-13812 y CVE-2018-13813:
    - Restringir el acceso a la red donde se encuentran los servidores web afectados.
    - Desactivar el servidor web si no se está utilizando. El servidor web está deshabilitado por defecto.

Siemens ha publicado parches y actualizaciones para todos los productos afectados por las siguientes vulnerabilidades:

- CVE-2018-13814:
    - Paneles SIMATIC HMI 4" - 22", Paneles SIMATIC HMI Comfort Outdoor 7" y 15", Paneles móviles SIMATIC HMI KTP KTP400F, KTP700, KTP700F, KTP900 y KTP900F: Actualizar SIMATIC WinCC (TIA Portal) a la versión V15 Update 4 o superior y luego actualizar el panel a la versión V15 Update 4 o superior.
    - SIMATIC WinCC Runtime Advanced, SIMATIC WinCC Runtime Professional, SIMATIC WinCC Runtime Professional y SIMATIC WinCC Runtime Professional:Actualizar a la versión V15 Update 4 o superior.
- CVE-2018-16555:
    - Para los dispositivos SCALANCE S602, SCALANCE S612, SCALANCE S623 y SCALANCE S627-2M Siemens recomienda actualizar a la versión 4.0.1.1.
- CVE-2018-13815:
    - S7-1500: actualizar a la versión 2.6.
    - S7-1200: seguir las siguientes pautas:
        - Proteger el acceso de red al puerto 102/tcp de los dispositivos afectados.
        - Aplicar el concepto de protección de celda.
        - Aplicar defensa en profundidad.
- CVE-2018- 13811:
    - SIMATIC STEP 7: actualizar a la versión 15.1
- CVE-2018-13804:
    - Siemens ha publicado la actualización de la versión 7.1 Upd3 para SIMATIC IT Production Suite
    - Siemens ha publicado la versión 2.4 de SIMATIC IT UA Discrete Manufacturing

Detalle:

La explotación exitosa de alguna de estas vulnerabilidades podría derivar en:

- **Denegación de servicio:** Se han asignado los identificadores CVE-2018-16556 y CVE-2018-16557 para estas vulnerabilidades.
- **Salto de directorio:** Se ha asignado el identificador CVE-2018-13812 para esta vulnerabilidad.
- **Redirecciones a URL no controladas:** Se ha reservado el identificador CVE-2018-13813 para esta vulnerabilidad.
- **Inyección de cabeceras HTTP:** Se ha reservado el identificador CVE-2018-13814 para esta vulnerabilidad.
- **Cross-Site Scripting (XSS):** Se ha asignado el identificador CVE-2018-16555 para esta vulnerabilidad.
- **Denegación de servicio:** Se ha asignado el identificador CVE-2018-13813 para esta vulnerabilidad.
- **Contraseñas almacenadas con hash débil:** Se ha asignado el identificador CVE-2018-13811 para esta vulnerabilidad.
- **Evasión de autenticación:** Se ha asignado el identificador CVE-2018-13804 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Siemens, Vulnerabilidad

---

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

Fecha de publicación: 14/11/2018

Importancia: Alta

Recursos afectados:

Todas las variantes de los siguientes productos CODESYS V3 en todas las versiones anteriores a la V3.5.13.20 que contienen el componente CmpTraceMgr se ven afectados, 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 RTE V3.
- CODESYS Control RTE V3 (para Beckhoff CX).
- CODESYS Control Win V3 (también parte de la configuración de CODESYS Development System).
- CODESYS V3 Simulation Runtime (parte del CODESYS Development System).
- CODESYS Control V3 Runtime System Toolkit.

El componente CmpOpenSSL se lanzó inicialmente con la versión V3.5.5.0. En general, todos los sistemas de tiempo de ejecución de CODESYS V3 anteriores a la versión V3.5.13.20, que contengan el componente CmpOpenSSL y que se ejecuten sobre uno de los siguientes sistemas operativos se ven afectados:

- Linux
- WindowsCE

Todas las variantes de los siguientes productos CODESYS V3 en todas las versiones anteriores a la V3.5.13.30 que contienen el componente CmpBlkDrvTcp se ven afectados, independientemente del tipo de CPU o sistema operativo:

- Todos los que afectaban al componente CmpTraceMgr, salvo 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 Gateway V3.
- CODESYS HMI V3.
- CODESYS OPC Server V3.
- CODESYS PLCHandler SDK.
- CODESYS Development System V3.

Descripción:

Los investigadores de ABB Switzerland Ltd., Jérôme Vialle de Schneider Electric y los clientes OEM del producto CODESYS, han reportado varias vulnerabilidades de denegación de servicio. Un potencial atacante remoto podría aprovechar estas vulnerabilidades, causando una falta de disponibilidad de los productos afectados.

Solución:

3S-Smart Software Solutions GmbH ha publicado nuevas versiones (V3.5.12.70 y V3.5.13.20) para solventar las vulnerabilidades que afectan a los productos de CODESYS, que pueden obtenerse desde su centro de descarga.

Detalle:

- El envío de una petición especialmente diseñada en las comunicaciones del producto afectado, podría permitir a un atacante remoto un acceso no permitido en CODESYS, provocando la denegación de servicio.
- Un atacante remoto podría crear peticiones TLS para impedir que los clientes puedan comunicarse con los servidores mediante el uso del componente CmOpenSSL de CODESYS Control runtime system, provocando la denegación del servicio.
- El envío de paquetes TCP especialmente diseñados podría permitir a un atacante remoto bloquear las comunicaciones entre clientes TCP de CODESYS y CODESYS Control runtime system, provocando la denegación del servicio.

Etiquetas: Comunicaciones, Vulnerabilidad

Desbordamiento de búfer en Sherlock de Teledyne DALSA

Fecha de publicación: 21/11/2018

Importancia: Alta

Recursos afectados:

- Sherlock versiones 7.2.7.4 y anteriores

Descripción:

El investigador Robert Hawes ha identificado una vulnerabilidad de desbordamiento de búfer en el interfaz de visión artificial Sherlock que podría permitir a un atacante la ejecución remota de código.

Solución:

Teledyne DALSA recomienda actualizar Sherlock a la versión 7.2.7.5 o posterior.

Detalle:

- Un atacante podría provocar un desbordamiento de búfer que le permitiría ejecutar código de forma remota y bloquear el dispositivo afectado. Se ha reservado el identificador CVE-2018-17930 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Schneider Electric

Fecha de publicación: 27/11/2018

Importancia: Media

Recursos afectados:

- PLC modelos Modicon M340, Premium, Quantum y BMXNOR0200.

Descripción:

El investigador Jacob Baines de Tenable ha identificado varias vulnerabilidades de cambio de contraseña no verificado y validación de datos inadecuada que afectan a varios productos de Schneider Electric que podrían provocar que un atacante remoto no autenticado pueda ver, modificar y borrar contraseñas u ocasionar una denegación de servicio.

Solución:

Schneider Electric recomienda seguir las instrucciones recogidas en el manual de referencia *Modicon Controllers Platform Cyber Security*.

Como prevención, el servidor web está deshabilitado por defecto, debido a que los servicios web solo son necesarios para tareas concretas de monitorización, configuración y mantenimiento. Si se habilitan para estas tareas, deberían deshabilitarse en el momento que no sean necesarios.

Adicionalmente se recomienda a los usuarios:

- Configurar listas de control de acceso para restringir el acceso al servidor web a las direcciones IP autorizadas.
- Proteger el acceso a los productos Modicon con cortafuegos.

Detalle:

- Un atacante podría acceder a la función de cambio de contraseña del servidor web embebido sin la correspondiente verificación. Se ha reservado el identificador CVE-2018-7811 para esta vulnerabilidad.
- La inadecuada verificación en el acceso a la función de borrado de contraseña del servidor web embebido podría permitir a un atacante remoto no autenticado acceder a ella. Se ha reservado el identificador CVE-2018-7809 para esta vulnerabilidad.
- Un atacante podría modificar, mediante un XSS, una URL con código JavaScript que será ejecutado dentro del navegador del usuario y afectar al dispositivo que está ejecutando dicho navegador. Se ha reservado el identificador CVE-2018-7810 para esta vulnerabilidad.

- Mediante el envío de una URL manipulada a un usuario autenticado se lograría cambiar la contraseña en el servidor. Se ha reservado el identificador CVE-2018-7831 para esta vulnerabilidad.
- El envío de una petición HTTP especialmente modificada mediante una neutralización inadecuada de secuencias CRLF en cabeceras HTTP podría provocar una denegación de servicio de, aproximadamente, 1 minuto de duración por parte del atacante. Se ha reservado el identificador CVE-2018-7830 para esta vulnerabilidad.

Etiquetas: Schneider Electric, Vulnerabilidad

Múltiples vulnerabilidades en el subsistema adicional GNU/Linux del SIMATICS S7-1500 CPU 1518(F)-4 PN/DP MFP de Siemens

Fecha de publicación: 28/11/2018

Importancia: Alta

Recursos afectados:

- Subsistema adicional de GNU/Linux, versión de firmware V2.6.0 para el SIMATICS S7-1500 CPU 1518(F)-4 PN/DP MFP.

Descripción:

Siemens ha identificado una serie de vulnerabilidades que afectan al subsistema adicional de GNU/Linux presente en su dispositivo SIMATICS S7-1500 CPU 1518(F)-4 PN/DP MFP. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante originar una denegación de servicio, obtener información de los usuarios o ejecutar una escalada de privilegios.

Solución:

Actualmente, Siemens se encuentra trabajando en una actualización de firmware que solvente estas vulnerabilidades y, hasta que se encuentre disponible, recomienda:

- Aplicar el concepto Defensa en Profundidad.
- Compilar y ejecutar solo aplicaciones que provengan de fuentes confiables.

Detalle:

Siemens ha identificado las siguientes vulnerabilidades que afectan al subsistema adicional de GNU/Linux, asignando estos identificadores:

- Para las vulnerabilidades en tiempo de ejecución: CVE-2018-14404, CVE-2018-15473, CVE-2018-17182 y CVE-2018-17972.
- Para las vulnerabilidades en tiempo de compilación: CVE-2018-6543, CVE-2018-6759, CVE-2018-6872, CVE-2018-7208, CVE-2018-7568, CVE-2018-7569, CVE-2018-7570, CVE-2018-7642, CVE-2018-7643, CVE-2018-9138, CVE-2018-9996, CVE-2018-10534, CVE-2018-10535, CVE-2018-18605, CVE-2018-18606, CVE-2018-18607 y CVE-2018-18309.

Etiquetas: Siemens, Vulnerabilidad

Vulnerabilidad de validación incorrecta de datos de entrada en CP400 Panel Builder de ABB

Fecha de publicación: 29/11/2018

Importancia: Alta

Recursos afectados:

- CP400PB, Panel Builder para CP405 y CP408, versiones 2.0.7.05 y anteriores.

Descripción:

El investigador Iván Sánchez de Nullcode Team ha descubierto una vulnerabilidad de tipo validación incorrecta de datos de entrada en CP400 Panel Builder. Una explotación exitosa podría causar que el *Text Editor* de CP400PB se detenga e inserte y ejecute código arbitrario en el equipo donde se utiliza el *Text Editor*.

Solución:

Esta vulnerabilidad se ha corregido en las versiones 2.1.7.21 y posteriores.

Detalle:

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

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en VT-Designer de INVT Electric

Fecha de publicación: 30/11/2018

Importancia: Media

Recursos afectados:

- VT-Designer versión 2.1.7.31

Descripción:

Ariel Caltabiano, en colaboración con ZeroDay initiative de Trend Micro, ha reportado múltiples vulnerabilidades, que podrían permitir a un atacante remoto bloquear el programa o ejecutar código.

Solución:

- INVT Electric todavía no ha publicado una solución para estas vulnerabilidades

Detalle:

- Los objetos se completan con la información suministrada por el usuario a través de un archivo, sin haber comprobado previamente su validez, lo que podría permitir al atacante escribir información en ubicaciones de memoria conocidas, pudiendo bloquear el programa o ejecutar código de forma remota. Se ha reservado el identificador CVE-2018-18987 para esta vulnerabilidad.
- El programa lee el contenido de un archivo que ya está en memoria en otro búfer basado en memoria dinámica (heap), lo que podría permitir el bloqueo del programa o la ejecución remota de código. Se ha reservado el identificador CVE-2018-18983 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Vulnerabilidad de inyección de comandos en NPort W2x50A de Moxa

Fecha de publicación: 30/11/2018

Importancia: Alta

Recursos afectados:

- Moxa NPort W2x50A versiones de firmware 2.1 Build_17112017 y anteriores.

Descripción:

Se ha descubierto una vulnerabilidad de inyección de comandos en Moxa NPort V2x50A, un atacante podría inyectar comandos de sistema y conseguir ejecución de código.

Solución:

- Actualizar NPort W2x50A a la versión 2.2 Build_18082311 o posterior.

Detalle:

- Un atacante autenticado en el servidor web podría inyectar comandos de sistema en las peticiones *ping* o *wlan profile* y enviar un paquete POST especialmente diseñado a */goform/net_WebPingGetValue* o a */goform/net_WebSettingProfileSecurity*, y conseguir la ejecución de código. Se han reservado los identificadores CVE-2018-19659 y CVE-2018-19660 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad