Boletín de mayo de 2019

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en CompactLogix y GuardLogix de Rockwell Automation

Fecha de publicación: 02/05/2019

Importancia: Alta

Recursos afectados:

- Controladores CompactLogix 5370 L1 versiones de la 20 a la 30.014 y anteriores;
- Controladores CompactLogix 5370 L2 versiones de la 20 a la 30.014 y anteriores;
- Controladores CompactLogix 5370 L3 versiones de la 20 a la 30.014 y anteriores;
- Controladores Compact GuardLogix 5370 versiones de la 20 a la 30.014 y anteriores;
- Controladores Armor Compact GuardLogix 5370 versiones de la 20 a la 30.014 y anteriores.

Descripción:

Los investigadores, Younes Dragoni de Nozomi Networks y George Lashenko de CyberX, han reportado vulnerabilidades de tipo control inadecuado de recursos y desbordamiento de búfer, en los productos CompactLogix y GuardLogix de Rockwell Automation. La explotación exitosa de estas vulnerabilidades permitiría a un atacante remoto provocar una denegación de servicio del servidor web o provocar una falta no recuperable en los dispositivos (*MNRF*, del inglés *Major Non-Recoverable Fault*).

Solución:

- Rockwell Automation recomienda encarecidamente a los usuarios aplicar los últimos parches disponibles a los dispositivos, para estar al día con las últimas funcionalidades, corrección de errores y mejoras de seguridad. Actualizar a la versión de firmware FRN 31.011 o posteriores, mitiga los riesgos asociados a estas vulnerabilidades.

Detalle:

- Control inadecuado de recursos: un atacante remoto, puede enviar un paquete HTTP/HTTPS, especialmente diseñado, que aproveche una vulnerabilidad de desbordamiento de búfer, provocando la posibilidad de ejecutar código de forma remota o dejar el servidor no disponible. Sería necesario un reinicio forzado, *cold restart*,para recuperar el sistema. Se ha asignado el identificador CVE-2019-10952 para esta vulnerabilidad.
- Desbordamiento de búfer: un atacante remoto, puede enviar un paquete SNMP especialmente diseñado, para provocar una denegación de servicio que dejaría al controlador en un estado de falta mayor no recuperable (MNRF). Se ha asignado el identificador CVE-2019-10954 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en comunicadores de GE

Fecha de publicación: 03/05/2019

Importancia: Alta

Recursos afectados:

- Communicator Installer, Application, PostGreSQL, MeterManager y WISE Uninstaller, versiones anteriores a la 4.0.517.

Descripción:

El investigador Reid Wightman de Dragos ha reportado varias vulnerabilidades de tipo: ruta de búsqueda no controlada, uso de credenciales embebidas y control de acceso incorrecto. Un potencial atacante podría obtener permisos de administrador, manipular

widgets e interfaces de usuario, obtener el control de la base de datos o ejecutar comandos reservados para administración.

Solución:

- El fabricante recomienda actualizar los comunicadores a la versión 4.0.517 o superior.

Detalle:

- Un atacante sin permisos administrativos podría colocar archivos maliciosos en el directorio de archivos del instalador para obtener privilegios administrativos en un sistema durante la instalación o la actualización. Se ha reservado el identificador CVE-2019-6564 para esta vulnerabilidad.
- Un atacante podría colocar archivos maliciosos en el directorio de trabajo del programa para manipular widgets y elementos de la interfaz de usuario. Se ha reservado el identificador CVE-2019-6546 para esta vulnerabilidad.
- Existen dos cuentas de usuarios, consideradas backdoors, que podrían permitir el control sobre la base de datos por parte de un atacante. Este servicio es inaccesible para un atacante si la víctima usa la configuración predeterminada del cortafuegos de Windows. Se ha reservado el identificador CVE-2019-6548 para esta vulnerabilidad.
- Un servicio ejecutado con permisos del sistema, podría permitir a un atacante sin permisos realizar ciertas acciones administrativas, lo que puede permitir la ejecución de scripts programados con privilegios de administrador en el sistema. Este servicio es inaccesible para los atacantes si el usuario víctima usa la configuración predeterminada del cortafuegos de Windows. Se ha reservado el identificador CVE-2019-6544 para esta vulnerabilidad.
- Un atacante sin permisos de administración puede reemplazar el desinstalador con una versión maliciosa para obtener privilegios de administrador en el sistema. Se ha reservado el identificador CVE-2019-6566 para esta vulnerabilidad

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en SiteOmat de Orpak

Fecha de publicación: 03/05/2019

Importancia: Crítica

Recursos afectados:

- SiteOmat, versiones anteriores a la 6.4.414.122
- SiteOmat, versiones anteriores a la 6.4.414.084

Descripción:

El investigador Ido Naor de Kaspersky Lab ha reportado varias vulnerabilidades de tipo uso de contraseñas embebidas, *Cross-Site Scripting* (XSS), Inyección SQL, falta de cifrado en datos sensibles, inyección de código y desbordamiento de búfer. La explotación exitosa de estas vulnerabilidades permitiría a un atacante ejecutar código remoto originando una posible denegación de servicio y acceso no autorizado para ver y editar información de monitorización, configuración y pago.

Solución:

- El fabricante recomienda actualizar las versiones afectadas a la versión v6.4.414.139 o posterior. La actualización puede obtenerse contactando con el fabricante en la página de soporte de Orpak (requiere registro previo).

Detalle:

- Uso de contraseñas embebidas: la aplicación utiliza credenciales embebidas. Se ha reservado el identificador CVE-2017-14728 para esta vulnerabilidad.
- *Cross-Site Scripting* (XSS): la aplicación web no realiza un correcto filtrado de los parámetros de entrada, este hecho permite la explotación de *Cross-Site Scripting*. Se ha asignado el identificador CVE-2017-14850 para esta vulnerabilidad.
- Inyección SQL: la aplicación no realiza el correcto filtrado de los parámetros de entrada. Este hecho podría permitir a un atacante acceder a información del producto mediante la introducción de una entrada especialmente diseñada. Se ha reservado el identificador CVE-2017-14851 para esta vulnerabilidad.
- Falta de cifrado en datos sensibles: la aplicación envía información sensible en texto plano. Entre la información sensible enviada, se encuentran credenciales. Un atacante podría capturar las credenciales enviadas por red y saltarse la autenticación del producto afectado. Se ha reservado el identificador CVE-2017-14852 para esta vulnerabilidad.
- Inyección de código: la aplicación no restringe adecuadamente los parámetros de entrada externos. Este hecho permitiría a un atacante no autenticado ejecutar código especialmente diseñado en el sistema víctima. Se ha reservado el identificador CVE-2017-14853 para esta vulnerabilidad.
- Desbordamiento de búfer: la aplicación utiliza una función que acepta parámetros de entrada de usuarios. Dicha entrada no posee un correcto tratamiento por lo que un atacante podría ejecutar código arbitrario. Se ha reservado el identificador CVE-2017-14854 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en AirLink ALEOS de Sierra Wireless

Fecha de publicación: 03/05/2019

Importancia: Crítica

Recursos afectados:

- LS300, GX400, GX440 y ES440, versión 4.4.8 y anteriores.
- GX450 y ES450, versiones anteriores a la 4.9.4.
- MP70, MP70E, RV50, RV50X, LX40 y LX60, versiones anteriores a la 4.12.

Descripción:

Los investigadores Carl Hud y Jared Rittle, de Cisco Talos, han identificado varias vulnerabilidades de tipo inyección de comandos de SO, uso de credenciales embebidas, subida no restringida de ficheros peligrosos, *cross-site scripting* (XSS), *cross-site request forgery* (CSRF),

exposición de información, falta de encriptación en datos sensibles, cambio de contraseña no verificado y asignación de permisos incorrecta para recursos críticos que afectan a los productos AirLink ALEOS de Sierra Wireless. La explotación exitosa de estas vulnerabilidades permitiría a un atacante ejecutar código remoto, averiguar credenciales de usuario, subir archivos o descubrir rutas de fichero.

Solución:

El fabricante recomienda actualizar a las últimas versiones de ALEOS para los productos y versiones listadas a continuación (algunas aún no están disponibles):

- LS300, GX400, GX440, ES440: ALEOS 4.4.9 (disponible a finales de 2019).
- GX450, ES450: ALEOS 4.9.4.p09 (disponible actualmente).
- MP70, MP70E, RV50, RV50X, LX40, LX60: ALEOS 4.12 (disponible a finales de junio 2019).

Sierra Wireless recomienda, además, seguir las siguientes indicaciones:

- Asegurar el uso de una contraseña robusta.
- Si ALEOS Application Framework (AAF) está activado, asegurarse de que se usa una contraseña robusta para la cuenta de usuario AAF.
- Si se utiliza Telnet o SSH, asegurarse de que se usa una contraseña robusta para la cuenta de la consola.
- Al conectar directamente al ACEmanager:
  - Usar únicamente HTTPS.
  - Utilizar un navegador moderno y actualizado, como Chrome, Firefox o Edge.

Detalle:

- Una petición HTTP autenticada, especialmente diseñada, puede inyectar comandos arbitrarios, resultando en la ejecución remota de código. Se ha reservado el identificador CVE-2018-4061 para esta vulnerabilidad.
- La activación de SNMPD fuera del WebUI provocaría la activación de las credenciales codificadas, lo que resulta en la exposición de un usuario privilegiado. Un atacante puede activar SNMPD, sin ningún cambio de configuración, para explotar esta vulnerabilidad. Se ha reservado el identificador CVE-2018-4062 para esta vulnerabilidad.
- Una petición HTTP autenticada, especialmente diseñada, puede cargar un archivo, lo que resulta en una carga de código ejecutable y enrutable al servidor web. Se ha reservado el identificador CVE-2018-4063 para esta vulnerabilidad.
- Una petición HTTP, especialmente diseñada, puede causar un cambio de configuración de dispositivo no verificado, lo que resulta en un cambio no verificado de la contraseña de usuario en el dispositivo. Un atacante puede realizar una petición HTTP autenticada para explotar esta vulnerabilidad. Se ha reservado el identificador CVE-2018-4064 para esta vulnerabilidad.
- Una petición *ping* HTTP, especialmente diseñada, puede hacer que JavaScript reflejado se ejecute en el navegador del usuario. Un atacante puede explotar esta vulnerabilidad, engañando a un usuario para que haga clic en un enlace o URL incrustada que redirija a la vulnerabilidad de secuencias de comandos entre sitios reflejada. Se ha reservado el identificador CVE-2018-4065 para esta vulnerabilidad.
- Una solicitud HTTP, especialmente diseñada, puede hacer que un usuario autenticado realice solicitudes privilegiadas sin saberlo, lo que resulta en solicitudes no autenticadas a través de dicho usuario. El desencadenamiento de esta vulnerabilidad puede permitir que un atacante acceda a páginas autenticadas a través de un usuario identificado. Se ha reservado el identificador CVE-2018-4066 para esta vulnerabilidad.
- Una petición HTTP autenticada, especialmente diseñada, puede causar una fuga de información, lo que da lugar a la revelación de las rutas internas de los archivos. Se ha reservado el identificador CVE-2018-4067 para esta vulnerabilidad.
- Una petición HTTP puede dar lugar a la revelación de la configuración predeterminada del dispositivo. Un atacante puede enviar una petición HTTP no autenticada para explotar esta vulnerabilidad. Se ha reservado el identificador CVE-2018-4068 para esta vulnerabilidad.
- La funcionalidad de autenticación de ACEManager se realiza en texto plano XML al servidor web. Un atacante puede escuchar el tráfico de la red desde el dispositivo para aprovechar esta vulnerabilidad. Se ha reservado el identificador CVE-2018-4069 para esta vulnerabilidad.
- Una solicitud HTTP, especialmente diseñada, puede causar la revelación de información, lo que resulta en la exposición de información confidencial, incluyendo, pero no limitando a, contraseñas de texto plano y cadenas SNMP. Un atacante puede realizar una petición HTTP autenticada, o ejecutar el binario, para explotar esta vulnerabilidad. Se han reservado los identificadores CVE-2018-4070 y CVE-2018-4071 para esta vulnerabilidad.
- Una petición HTTP, especialmente diseñada, puede hacer que se escriba una configuración arbitraria, lo que resulta en cambios no verificados en cualquier configuración del sistema. Un atacante puede realizar una petición HTTP autenticada, o ejecutar el binario como cualquier usuario, para explotar esta vulnerabilidad. Se han reservado lps identificadores CVE-2018-4072 y CVE-2018-4073 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Control de accesos inadecuado en Video Recording Manager de Bosch

Fecha de publicación: 10/05/2019

Importancia: Crítica

Recursos afectados:

- Bosch Diver IP 5000 versiones 3.80.0033, 3.80.0035 y 3.80.0037.
- Bosch Video Recording Manager versiones 3.70.0056, 3.70.0058, 3.70.0060, 3.70.0062, 3.71.0022, 3.71.0029, 3.71.0031, 3.71.0032, 3.81.0032, 3.81.0038, 3.81.0048.
- Bosch Video Management System versiones 7.5 y 8.0, las cuales emplean las siguientes versiones vulnerables de VRM: 3.70.0056, 3.70.0058, 3.70.0060, 3.70.0062, 3.71.0022, 3.71.0029, 3.71.0031, 3.71.0032.
- Bosch Video Management System versión 9.0, la cual emplea las siguientes versiones vulnerables de VRM: 3.81.0032, 3.81.0038, 3.81.0048.

Descripción:

Bosch ha reportado una vulnerabilidad de tipo control de accesos inadecuado que afecta a su software Video Recording Manager (VRM) y que podría permitir a un atacante remoto sin autenticación el acceso a un subconjunto limitado de certificados.

Solución:

Para sus productos Bosch recomienda:

- Para DIVAR IP 5000 3.80, actualizar a la versión de firmware 3.80.0039

- Para Video Recording Manager:
  - versión 3.70, actualizar a la versión 3.71.0034.
  - versión 3.71, actualizar a la versión 3.71.0034.
  - versión 3.81, actualizar a la versión 3.81.0050.
- Para Bosch Video Management System:
  - versiones 7,5 y 8.0, actualizar VRM a 3.71.0034.
  - versión 9.0, actualizar VRM a 3.81.0050.

Detalle:

- Existe una vulnerabilidad de tipo control de acceso inadecuado que afecta al software Video Recording Manager de Bosch y que podría permitir a un atacante el acceso de manera remota y sin autenticación a un subconjunto de certificados almacenados en el sistema operativo. Se ha asignado el identificador CVE-2019-11684 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Siemens

Fecha de publicación: 14/05/2019

Importancia: Crítica

Recursos afectados:

- LOGO! Soft Comfort y BM, todas las versiones.
- SCALANCE W1750D, todas las versiones anteriores a la V8.4.0.1.
- SINAMICS PERFECT HARMONY GH180 con NXG I y NXG II control, MLFBs: 6SR2. . . -, 6SR3. . . -, 6SR4. . .-, todas las versiones con opción G28.
- SIMATIC PCS 7 V9.0, V8.2, V8.2 y V8.0 y anteriores, todas las versiones.
- SIMATIC WinCC (TIA Portal) V15, V14 y V13, todas las versiones.
- SIMATIC WinCC Runtime Professional, todas las versiones.
- SIMATIC WinCC V7.2 y anteriores, todas las versiones.
- SIMATIC WinCC V7.3 y posteriores, todas las versiones
- SIMATIC WinCC V7.4, V7.3 y V7.2, todas las versiones.
- SIMATIC WinCC V7.5, todas las versiones anteriores a la versión 7,5 Upd3.
- SIMATIC PCS 7 V8.0 y anteriores, todas las versiones.
- SIMATIC PCS 7 V8.1 y posteriores, todas las versiones.
- SIMATIC PCS V7.2 y todas las versiones anteriores.
- SIMATIC WinCC V7.3 y todas las versiones posteriores.
- SIMATIC HMI Comfort Panels 4" - 22". Todas las versiones anteriores a la V15.1 Update 1.
- SIMATIC HMI Comfort Outdoor Panels 7" & 15". Todas las versiones anteriores a la V15.1 Update 1.
- SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 und KTP900F. Todas las versiones anteriores a la V15.1 Update 1.
- SIMATIC WinCC Runtime Advanced, Professional y TIA Portal. Todas las versiones anteriores a la V15.1 Update 1.
- SIMATIC HMI Classic Devices (TP/MP/OP/MPMobile Panel). Todas las versiones.
- SISHIP EMCS, IMAC y IPMS: Todas las versiones.

Descripción:

Los investigadores Vladimir Dashchenko y Sergey Temnikov de Kaspersky Lab ICS CERT, ChengBin Wang de ZheJiang Guoli Security Technology, Manuel Stotz y Matthias Deeg de SySS GmbH y axt, la empresa iDefense Labs y el CNCERT/CC, además del propio Siemens, han identificado múltiples vulnerabilidades de tipo divulgación de información, corrupción de memoria, desbordamiento de búfer, configuración inadecuada, contraseñas embebidas, uso de cifrado inadecuado, XSS, comunicaciones en claro, error de carga de ficheros, inyección de comandos, etc., que afectan a diversos productos de Siemens. Un potencial atacante podría reiniciar el dispositivo, conseguir una situación de denegación de servicio, ejecutar comandos o la obtención de información sensible.

Solución:

- Para SCALANCE W1750D, actualizar a la nueva versión.
- Para SINAMICS PERFECT HARMONY GH180 Drives NXG I y NXG II actualizar a NXGpro control.
- Para SISHIP Automation de Siemens, actualizar a la versión aportada por WibuKey.
- Para SIMATIC WinCC (ITA Portal) y SIMATIC HMI, actualizar a V15.1 Update 1 o superior
- En cuanto a los dispositivos para los cuales Siemens no dispone de una nueva actualización, recomienda una serie de medidas de mitigación y buenas prácticas:
  - Abrir proyectos solamente provenientes de fuentes validadas.
  - Aplicar los conceptos de ciberseguridad descritos en los manuales.
  - Aplicar los principios de defensa en profundidad.
  - Establecer canales cifrados para las comunicaciones entre SIMATIC WinCC y SIMATIC PCS 7 '*Encrypted communication*'.
  - Restringir el acceso a los servicios web de los dispositivos afectados.
  - Restringir los accesos al puerto 161/UDP solamente a dispositivos validados.
  - Deshabilitar la funcionalidad de Lectura/Escritura en el parámetro de *Fieldbus*.

Detalle:

Las vulnerabilidades de severidad crítica son las siguientes:

- Un atacante no autenticado con acceso a la red donde se encuentra el dispositivo afectado por el puerto 10005/TCP, podría realizar acciones de reconfiguración y obtener ficheros de los proyectos que posea el dispositivo. Esta vulnerabilidad tiene impacto sobre la confidencialidad, integridad y disponibilidad del dispositivo afectado. Se ha reservado el identificador CVE-2019-10919 para esta vulnerabilidad.
- Un atacante con acceso al servicio web del dispositivo afectado, podría realizar inyecciones de comandos sin necesidad de estar autenticado lo que podría permitir la ejecución arbitraria de comandos en el sistema operativo del dispositivo afectado, pudiendo copiar ficheros, leer configuraciones, escribir ficheros, eliminar ficheros o reiniciar el dispositivo. Se ha asignado el identificador CVE-2018-7084 para esta vulnerabilidad.
- Un atacante con acceso local y permisos en el servidor que contiene la base de datos, podría realizar ejecuciones de comandos en el sistema. Esta vulnerabilidad tiene impacto sobre la confidencialidad, integridad y disponibilidad del sistema afectado. Se ha reservado el identificador CVE-2019-10916 para esta vulnerabilidad.
- Un atacante no autenticado con acceso a la red donde se encuentra el dispositivo afectado que no utiliza comunicaciones cifradas, podría realizar una ejecución de código arbitrario. Esta vulnerabilidad tiene impacto sobre la confidencialidad, integridad y disponibilidad del sistema afectado. Se ha reservado el identificador CVE-2019-10922 para esta vulnerabilidad.
- Un atacante podría enviar un paquete IRP (peticiones E/S), especialmente diseñado, que origine un desbordamiento de búfer,

desembocando en una corrupción de la memoria del kernel y en una escalada de privilegios en el sistema. Se ha asignado el identificador CVE-2018-3990 para esta vulnerabilidad.
- Un atacante podría enviar un paquete TCP, especialmente diseñado, que originen un desbordamiento de búfer y provocar una ejecución de código remoto. Se ha asignado el identificador CVE-2018-3991 para esta vulnerabilidad.

Los identificadores asignados para el resto de vulnerabilidades son: CVE-2019-10924, CVE-2019-10920, CVE-2019-10921, CVE-2018-7083, CVE-2018-16417, CVE-2018-7082, CVE-2019-6578, CVE-2019-10918, CVE-2019-6574, CVE-2018-7064, CVE-2019-6572, CVE-2019-6576, CVE-2019-6577, CVE-2019-10917 y CVE-2018-3989.

Etiquetas: Actualización, Comunicaciones, SCADA, Siemens, Vulnerabilidad

Ruta de búsqueda no validada en Network Configurator de DeviceNet de Omron

Fecha de publicación: 15/05/2019

Importancia: Alta

Recursos afectados:

- Network Configurator de DeviceNet Safety, versiones 3.41 y anteriores.

Descripción:

El investigador n0b0dy, junto con la NCCIC, han reportado una vulnerabilidad de tipo ruta de búsqueda no validada en la aplicación Network Configurator de DeviceNet Safety de Omron. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante ejecutar código arbitrario con los privilegios de la aplicación.

Solución:

Omron aún no ha lanzado la actualización que resuelve esta vulnerabilidad. Mientras tanto, recomienda aplicar algunas de las siguientes medidas para mitigarla:

- Eliminar o restringir los directorios listados en la variable de entorno PATH.
- Asegurarse de que solamente las cuentas de administrador poseen los permisos de escritura sobre los directorios del sistema.
- Operar los PC de Windows con usuarios estándar, utilizando las cuentas de administrador para casos específicos.
- Asegurarse de que no existen archivos no confiables dentro del directorio donde está instalada la aplicación.
- Confirmar que no existen archivos no confiables en el directorio, antes de ejecutar un archivo de proyecto en él, o bien moverlo a una carpeta confiable.

Detalle:

- La aplicación utiliza recursos en una ruta de búsqueda no validada, que permitiría la ejecución de un archivo DLL malicioso ubicado en un lugar no controlado por la aplicación y fuera de los directorios previstos. Se ha reservado el identificador CVE-2019-10971 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en productos Schneider Electric

Fecha de publicación: 16/05/2019

Importancia: Alta

Recursos afectados:

- Modicon M580, con *firmware* anterior a V2.50, a V2.80 y a V2.30.
- Modicon M340, todas las versiones, con *firmware* anterior a V3.01.
- BMxCRA312XX, con *firmware* anterior a V2.40.
- Modicon Premium, todas las versiones.
- 140CRA312xxx, todas las versiones.
- Modicon Quantum, todas las versiones de *firmware* en versiones anteriores a V2.40.
- TSXETG100, todas las versiones.
- BMX-NOR-0200H, con *firmware* anterior a V1.7 IR 19.
- Floating License Manager, version V2.3.0.0 y anteriores.
- Modicon M100, todas las versiones.
- Modicon M200, todas las versiones.
- ATV IMC drive controller, todas las versiones.
- Modicon M241, todas las versiones.
- Modicon M251, todas las versiones.
- Modicon M258, todas las versiones.
- Modicon LMC058, todas las versiones.
- Modicon LMC078, todas las versiones.
- PacDrive Eco, todas las versiones.
- PacDrive Pr, todas las versiones.
- PacDrive Pro2, todas las versiones.
- NET55XX Enconder, con versión de *firmware* anterior a 2.1.9.7.

Descripción:

Varios investigadores de las compañías Positive Technologies, VAPT Team (C3i IITK, UP, India), CNCERT/CC, Fortiphyd Logic y Claroty, junto con Schneider Electric, han publicado múltiples vulnerabilidades de tipo denegación de servicio, inyección de código, Cross-Site Scripting (XSS), credenciales embebidas, valores insuficientemente aleatorios y falta de autenticación en función crítica que afectan a

diversos productos de Schneider Electric. Un atacante podría causar una condición de denegación de servicio, ejecutar scripts en el contexto del usuario, acceso sin autorización al servicio FTP, realizar un secuestro de la conexión TCP y modificar la configuración IP del dispositivo, y provocar un impacto en la confidencialidad, integridad y disponibilidad del producto.

Solución:

- Modicon M580: actualizar a la versión V2.80.
- Modicon M340: actualizar a la versión V3.01.
- BMX/E CRA: actualizar a la versión V2.40.
- Modicon Quantum: actualizar a la versión V3.5x.
- BMX-NOR-0200H: actualizar a la versión V1.7 IR19.
- Floating License Manager: actualizar a la versión V2.3.1.0.
- NET55XX Encoder: actualizar a la versión 2.1.9.7.

Para lo dispositivos que no disponen de actualización Schneider recomienda:

- Realizar una segmentación de red y bloquear los puertos TCP 502 y 4418 y los puertos UDP 2222, 27126 y 27127 en el cortafuegos.
- Utilizar un cortafuegos de aplicación para comprobar los datos de entrada de los usuarios o utilizar un cortafuegos estándar para limitar el tráfico HTTP y los accesos sin autorización al producto TSXETG100.
- Bloquear todo el tráfico externo a los puertos TCP en el cortafuegos y configurar una lista de control de acceso.
- Desactivar la opción 'Auto Discovery protocol enable'.
- Desactivar la opción 'Discovery protocol active'.

Detalle:

Las vulnerabilidades de severidad crítica son las siguientes:

- Un atacante remoto, mediante control de acceso incorrecto, podría comprometer la confidencialidad, integridad y disponibilidad al enviar una solicitud maliciosa a la webUI. Se ha reservado el identificador CVE-2019-6814 para esta vulnerabilidad.
- Un atacante remoto podría ejecutar código arbitrario en el componente Imadmin y Daemon de FlexNet Publisher, modificando la memoria asignada o desasignada y pudiendo provocar el cierre forzoso del Daemon. Se ha reservado el identificador CVE-2018-20033 para esta vulnerabilidad.

Las vulnerabilidades de severidad alta son las siguientes:

- La ausencia de autentificación en una función crítica podría permitir a un atacante la modificación de la configuración IP del dispositivo afectado (dirección IP, máscara de red o dirección IP de pasarela) al recibir una trama Ethernet específica. Se ha reservado el identificador CVE-2019-6820 para esta vulnerabilidad.
- Un atacante remoto podría causar una denegación de servicio, enviando un mensaje al componente Imadmin o el Daemon de FlexNet Publisher, pudiendo provocar el cierre forzoso del Daemon. Se han reservado los identificadores CVE-2018-20034, CVE-2018-20031 y CVE-2018-20032 para estas vulnerabilidades.
- Un atacante podría causar una denegación de servicio al usar una conexión telnet, aprovechando una vulnerabilidad en la administración de credenciales. Se ha reservado el identificador CVE-2018-7788 para esta vulnerabilidad.
- Un atacante podría causar una denegación de servicio o modificaciones no autorizadas en la configuración del PLC usando el protocolo Ethernet/IP, aprovechando una vulnerabilidad en los permisos, privilegios y control de acceso. Se ha reservado el identificador CVE-2018-6815 para esta vulnerabilidad.
- Un atacante podría inyectar código y causar una posible modificación no autorizada del *firmware* y la denegación del servicio al usar el protocolo Modbus. Se ha reservado el identificador CVE-2018-6816 para esta vulnerabilidad.
- Mediante la verificación inadecuada de condiciones inusuales, un atacante podría causar una denegación de servicio al enviar tramas Modbus específicas al controlador. Se ha reservado el identificador CVE-2018-6819 para esta vulnerabilidad.

Los identificadores asignados para el resto de las vulnerabilidades son: CVE-2018-7851, CVE-2018-7834, CVE-2018-6812 y CVE-2018-6821.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Lectura fuera de límites en Alpha7 PC Loader de Fuji Electric

Fecha de publicación: 17/05/2019

Importancia: Baja

Recursos afectados:

- Alpha7 PC Loader, versión 1.1 y anteriores.

Descripción:

El investigador de seguridad kimiya, de 9SG Security Team, en colaboración con Zero Day Initiative de Trend Micro, ha reportado esta vulnerabilidad de tipo lectura fuera de límites. La explotación exitosa de esta vulnerabilidad, permitiría a un atacante causar un funcionamiento erróneo en el dispositivo afectado.

Solución:

- El fabricante recomienda actualizar el software del dispositivo afectado a la versión 1.2 que permite solventar esta vulnerabilidad.

Detalle:

- La explotación exitosa de esta vulnerabilidad, de lectura fuera de límites, permitiría a un atacante generar un comportamiento incorrecto del dispositivo, provocando un cierre inesperado del sistema. Se ha reservado el identificador CVE-2019-10975 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en librería CAPICOM afecta a productos Yokogawa

Fecha de publicación: 17/05/2019

Importancia: Crítica

Recursos afectados:

- CENTUM:
  - CENTUM VP (R5.02.00 - R6.04.00)
  - CENTUM VP Entry Class (R5.02.00 - R6.04.00)
- STARDOM (R3.20 - R4.20)
- B/M9000 VP (R7.02.01 - R8.02.02)

Descripción:

Yokogawa ha identificado el uso de la librería CAPICOM en algunos de sus productos. Esta librería criptográfica contiene una vulnerabilidad que un atacante podría explotar para ejecutar código remoto.

Solución:

- El fabricante recomienda eliminar la librería CAPICOM para solucionar este problema de seguridad.

Detalle:

- La librería criptográfica CAPICOM tiene asociada una vulnerabilidad que podría permitir a un atacante realizar ejecución de código remoto. Se ha asignado el identificador CVE-2007-0940 a esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Vulnerabilidad de Microsoft Windows RDS (Remote Desktop Service) en Sistemas de Control Industrial

Fecha de publicación: 20/05/2019

Importancia: Crítica

Recursos afectados:

Varios fabricantes de productos de Sistemas de Control Industrial se han visto afectados por esta vulnerabilidad en el servicio RDS, entre ellos:

- Varios productos de la gama Siemens Healthineers.
- Varios productos de Schneider Electric que utilizan Microsoft Windows como sistema operativo.

Descripción:

La publicación de las actualizaciones de seguridad de Microsoft, publicadas este mes de mayo, describe una vulnerabilidad que afecta al servicio de RDS (*Remote Desktop Service*), que afectaría a varios productos industriales que utilizan este servicio en sus productos, como la gama de Siemens Healthineers y varios productos de Schneider Electric. Esta vulnerabilidad permitiría a un atacante remoto no autenticado, la ejecución de código remoto en el sistema objetivo, si este sistema tiene accesible a la red el servicio de RDS (*Remote Desktop Service*) de Microsoft Windows. Este aviso ya fue publicado en INCIBE-CERT para sistemas de TI, como Boletín de seguridad de Microsoft de mayo de 2019.

Solución:

- Microsoft dispone de actualización para los sistemas operativos afectados, que soluciona la vulnerabilidad en RDS (*Remote Desktop Service*).

Detalle:

- La vulnerabilidad encontrada en el servicio RDS (*Remote Desktop Service*) de Microsoft Windows, podría permitir a un atacante remoto no autenticado ejecutar código. El atacante debe disponer de acceso a la red, y el sistema debe tener el servicio RDS expuesto, generalmente por el puerto 3389/TCP. El envió de peticiones RDP especialmente diseñadas, permitiría al atacante explotar esta vulnerabilidad, que entre otras acciones podría instalar programas, crear cuentas o ejecutar código de forma remota. Se ha asignado el identificador CVE-2019-0708 para esta vulnerabilidad.

Etiquetas: Actualización, Microsoft, Schneider Electric, Siemens, Vulnerabilidad, Windows

---

Vulnerabilidad en productos Intel afecta a Sistemas de Control Industrial

Fecha de publicación: 20/05/2019

Importancia: Alta

Recursos afectados:

- Este es el listado de CPUs afectadas proporcionado por Intel.

Fabricantes de productos de sistemas de control industrial se han visto afectados por estas vulnerabilidades en CPUs, entre ellos:

- Schneider Electric.

Descripción:

Diversos productos están afectados por una vulnerabilidad de seguridad que afecta a una amplia gama de CPU de Intel. La explotación exitosa de esta vulnerabilidad permitiría a un atacante acceso a información sensible de otros procesos o con otros privilegios. Este aviso ya fue publicado en INCIBE-CERT para sistemas de TI, como Múltiples vulnerabilidades en productos de Intel.

Solución:

- Actualizar a la última versión de producto en el centro de descarga de software de Intel.

Detalle:

- La vulnerabilidad Microarchitectural Data Sampling (MDS), también denominada ZombieLoad, FallOut o RIDL, podría permitir a un atacante con permisos de ejecución de código en un sistema local, explotar esta vulnerabilidad para acceder a datos del sistema protegidos o para los que no debería tener acceso. Se han asignado los siguientes identificadores CVE-2018-12126, CVE-2018-12130, CVE-2018-12127, CVE-2019-11091 para esta vulnerabilidad.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Múltiples vulnerabilidades en XGW 3000 ZigBee Gateway de Miele

Fecha de publicación: 21/05/2019

Importancia: Media

Recursos afectados:

- XGW 3000 ZigBee Gateway.

Descripción:

El investigador Maxim Rupp ha reportado dos vulnerabilidades, de tipo CSRF (*Cross-site request forgery*) y omisión de autenticación, en el producto XGW 3000 ZigBee Gateway de Miele.

Solución:

- Instalar la versión de software 2.4.0 mediante la función de actualización automática de XGW 3000 ZigBee Gateway.

Detalle:

- Un sitio web malicioso visitado por un usuario administrativo autenticado, o un correo malicioso, pueden realizar cambios arbitrarios en el *admin panel* mediante un ataque CSRF.
- En combinación con la vulnerabilidad anterior, la contraseña de administrador se puede cambiar sin comprobar la antigua, omitiendo de esta manera la función de cambio de contraseña.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Modicon de Schneider Electric

Fecha de publicación: 21/05/2019

Importancia: Crítica

Recursos afectados:

- Modicon M580
- Modicon M340
- Modicon Quantum
- Modicon Premiun

Descripción:

El investigador, Jared Rittle, de Cisco Talos, junto con Schneider Electric han publicado varias vulnerabilidades de tipo violación de límite de confianza, denegación de servicio, revelación de información, autenticación inadecuada por suplantación, control de acceso incorrecto, entradas no confiables y lectura fuera de límites. Un atacante podría causar una condición de denegación de servicio, acceso sin autorización, provocar un impacto en la confidencialidad, integridad y disponibilidad del dispositivo.

Solución:

- **Modicon M580:** se liberará un parche a lo largo del Q3 de 2019 a través de la nueva versión de *firmware* 2.90, para algunas de las vulnerabilidades listadas. Para otras, ya existe un parche a partir de la 2.80, por lo que se recomienda actualizar a dicha versión. Existe una vulnerabilidad para la que no hay parche programado. Se deben seguir las siguientes recomendaciones para mitigar las debilidades de Modbus, mientras no existan parches:
  - Implementar segmentación de red y bloquear mediante un *firewall* todos los accesos no autorizados al puerto 502/TCP.
  - Configurar una comunicación segura siguiendo la siguiente guía.
  - Usar un módulo BMENOC y seguir las instrucciones para configurar la funcionalidad IPsec, tal y como se describe en la siguiente guía.
- **Modicon M340:** se liberará un parche a lo largo del Q3 de 2019, a través de la nueva versión de *firmware* 3.10, para algunas de las vulnerabilidades listadas. Para otras, ya existe un parche a partir de la 3.01, por lo que se recomienda actualizar a dicha versión. Existe una vulnerabilidad para la que no hay parche programado. Se deben seguir las siguientes recomendaciones para mitigar las debilidades de Modbus, mientras no existan parches:

    - Implementar segmentación de red y bloquear mediante un *firewall* todos los accesos no autorizados al puerto 502/TCP.
    - Configurar un ACL siguiendo las recomendaciones de la siguiente guía.
- **Modicon Premium:** se liberará un parche a lo largo del Q1 de 2020, a través de la nueva versión de *firmware* 3.20, para algunas de las vulnerabilidades listadas. Para otras, no está previsto la liberación de un parche, por lo que se deben seguir las siguientes recomendaciones para mitigar las debilidades de Modbus, mientras no existan parches:
    - Implementar segmentación de red y bloquear mediante un *firewall* todos los accesos no autorizados al puerto 502/TCP.
    - Configurar un ACL siguiendo las recomendaciones de la siguiente guía.
- **Modicon Quantum:** se liberará un parche a lo largo del Q1 de 2020, a través de la nueva versión de *firmware* 3.60, para algunas de las vulnerabilidades listadas. Para otras, no está previsto la liberación de un parche, por lo que se deben seguir las siguientes recomendaciones para mitigar las debilidades de Modbus mientras no existan parches:
    - Implementar segmentación de red y bloquear mediante un *firewall* todos los accesos no autorizados al puerto 502/TCP.
    - Configurar un ACL siguiendo las recomendaciones de la siguiente guía.

Detalle:

Un atacante podría:

- Causar un acceso no autorizado al realizar un ataque de fuerza bruta en el protocolo Modbus, debido a una violación de los límites de confianza. Se ha reservado el identificador CVE-2018-7846 para esta vulnerabilidad.
- Provocar una denegación de servicio debido a una verificación incorrecta de la integridad de los datos al enviar un archivo, al leer bloques de memoria con un tamaño no válido, enviar diversos parámetros no válidos, escribir variables fuera de límites y escribir variables de aplicación sensibles a través de Modbus. Se han reservado los identificadores CVE-2018-7849, CVE-2018-7843, CVE-2018-7853, CVE-2018-7853, CVE-2018-7854, CVE-2018-7855, CVE-2018-7856, CVE-2018-7857, CVE-2019-6807 para esta vulnerabilidad.
- Originar una escalada de privilegios al llevar a cabo un ataque de fuerza bruta. Se ha reservado el identificador CVE-2018-7842 para esta vulnerabilidad.
- Mediante control de acceso incorrecto, podría causar una denegación de servicio o la ejecución remota de código (RCE) al sobrescribir los ajustes de configuración. Se han reservado los identificadores CVE-2018-7847 y CVE-2019-6808 para esta vulnerabilidad.
- Mediante la lectura fuera de límite, podría provocar una divulgación de datos no esperados al leer bloques de memoria específicos. Se ha reservado el CVE-2018-7845 para esta vulnerabilidad.
- Causar la muestra de información no válida en el software Unity Pro, debido a entradas no confiables. Se ha reservado el CVE-2018-7850 para esta vulnerabilidad.

Etiquetas: 0day, Actualización, Schneider Electric, Vulnerabilidad

---

Consumo de recursos no controlado en MELSEC-Q Series de Mitsubishi Electric

Fecha de publicación: 22/05/2019

Importancia: Alta

Recursos afectados:

- Módulo de Ethernet QJ71E71-100 de MELSEC-Q Series, con número de serie 20121 y anteriores.

Descripción:

Los investigadores Younes Dragoni y Alessandro Di Pinto, de Nozomi Networds, han reportado una vulnerabilidad de tipo consumo de recursos no controlado. La explotación exitosa de esta vulnerabilidad, por parte de un atacante, puede hacer que el dispositivo no responda, teniendo que reiniciar físicamente el PLC.

Solución:

- El fabricante recomienda actualizar el módulo QJ71E71-100 a la versión de *firmware* 20122 para solventar esta vulnerabilidad.

Detalle:

- Un atacante podría enviar paquetes TCP, específicamente diseñados, contra el servicio FTP, forzando a los dispositivos de destino a entrar en un modo de error y provocar una condición de denegación de servicio. Se ha reservado el CVE-2019-10977 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Almacenamiento de credenciales inseguro en Vijeo Citect y CitectSCADA de Aveva

Fecha de publicación: 29/05/2019

Importancia: Media

Recursos afectados:

- Vijeo Citect, versiones 7.30 y 7.40
- CitectSCADA, versiones 7.30 y 7.40

Descripción:

El equipo VAPT y el centro C3i IIT Kanpur (India) han reportado esta vulnerabilidad de tipo protección insuficiente de contraseñas. Un atacante con acceso al sistema afectado podría consultar las contraseñas almacenadas en texto plano y utilizarlas para realizar acciones maliciosas.

Solución:

- El fabricante recomienda actualizar las versiones afectadas a CitectSCADA 2018 lo antes posible.

Detalle:

- Las versiones afectadas por la vulnerabilidad de almacenamiento de credenciales inseguro, guardan en memoria las contraseñas en texto claro. Un atacante con los permisos adecuados y acceso al sistema afectado, podría consultar las contraseñas almacenadas y utilizarlas para realizar acciones maliciosas.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Ovation OCR400 Controller de Emerson

Fecha de publicación: 29/05/2019

Importancia: Media

Recursos afectados:

- Ovation OCR400 Controller, ejecutando Ovation versión 3.3.1 o anteriores.

Descripción:

VDLab, una colaboración entre Venustech y Dongfang Electric Corporation (DEC), han reportado estas vulnerabilidades de tipo desbordamiento de búfer. La ejecución exitosa de estas vulnerabilidades, por parte de un atacante remoto, podría permitir la ejecución de código remoto o una escalada de privilegios en el sistema afectado.

Solución:

- Emerson, recomienda actualizar los dispositivos afectados a la última versión disponible. En el caso contrario, consultad la sección "Referencias" para más información.

Detalle:

- Una vulnerabilidad se debe a una gestión incorrecta por parte del comando LIST en el servicio FTP cuando recibe un nombre de archivo largo. Un atacante remoto podría realizar una sobreescritura de búfers que ocasionaría una ejecución de código y una escalada de privilegios. Se ha asignado el identificador CVE-2019-10967 para esta vulnerabilidad.
- Una vulnerabilidad de desbordamiento de búfer basado en memoria dinámica (heap), se debe a una gestión incorrecta en el servicio FTP cuando recibe un comando largo. Un atacante remoto podría realizar una corrupción de memoria que interrumpiría al controlador, una ejecución de código o una escalada de privilegios. Se ha asignado el identificador CVE-2019-10965 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad