Boletín de marzo de 2020

Avisos de Sistemas de Control Industrial

Autorización inapropiada en múltiples productos de B&R Industrial Automation GmbH

Fecha de publicación: 21/02/2020

Importancia: Crítica

Recursos afectados:

- Automation Studio, versiones:
  - 2.7;
  - 3.0.71;
  - 3.0.80;
  - 3.0.81;
  - 3.0.90;
  - desde 4.0.x hasta 4.6.4;
  - 4.7.2.
- Automation Runtime, versiones:
  - 2.96;
  - 3.00;
  - 3.01;
  - 3.06;
  - 3.07;
  - desde 3.08 hasta 3.10;
  - desde 4.00 hasta 4.03;
  - desde 4.04 hasta 4.03;
  - desde 4.04 hasta 4.63;
  - 4.72 y superiores.

Descripción:

Yehuda Anikster y Amir Preminger, de Claroty, han reportado una vulnerabilidad, de severidad crítica, de tipo autorización inapropiada, que afecta a varios productos de B&R Industrial Automation GmbH.

Solución:

B&R informa que, por razones técnicas del producto, no permiten el cambio de credenciales del SNMP. Para reducir el riesgo de esta vulnerabilidad, las siguientes versiones de Automation Studio desactivan el servicio SNMP por defecto en los proyectos AS recién creados:

- AS 4.6.5 (fecha de publicación prevista: 27/03/2020) y superiores;
- AS 4.7.3 (fecha de publicación prevista: 10/04/2020) y superiores;
- AS 4.8.2 (fecha de publicación prevista: 11/06/2020) y superiores.

Detalle:

Los productos afectados son vulnerables a una debilidad en el servicio SNMP, lo que permitiría a un atacante remoto, no autenticado, modificar la configuración de los dispositivos afectados. Se ha reservado el identificador CVE-2019-19108 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

Autenticación incorrecta en múltiples productos de Moxa

Fecha de publicación: 03/03/2020

Importancia: Alta

Recursos afectados:

- MGate MB3180 Series, versión de *firmware* 1.8 o anteriores;
- MGate MB3280 Series, versión de *firmware* 2.8 o anteriores;
- MGate MB3480 Series, versión de *firmware* 2.6 o anteriores;
- MGate MB3170 Series, versión de *firmware* 2.5 o anteriores;
- MGate MB3270 Series, versión de *firmware* 2.8 o anteriores.

Descripción:

Una vulnerabilidad, de tipo autenticación incorrecta, afecta a varios productos de la familia de Modbus TCP Gateways.

Solución:

- Para los productos de las series MB3180, MB3280 y MB3480, actualizar a la última versión de *firmware* correspondiente.
- Para los productos de las series MB3170 y MB3270, actualizar a la última versión de *firmware* correspondiente.

Detalle:

Se ha detectado una vulnerabilidad, de tipo autenticación incorrecta, que afecta a múltiples productos de Moxa. Esta vulnerabilidad permitiría a atacante remoto, no autenticado, eludir la autenticación, iniciando sesión con un nombre de usuario/contraseña vacío, y ejecutar acciones arbitrarias con privilegios de administrador en el sistema afectado.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Control de acceso inapropiado en ValveLink de Emerson

Fecha de publicación: 04/03/2020

Importancia: Alta

Recursos afectados:

ValveLink, versiones desde la v12.0.264 hasta la v13.4.118.

Descripción:

Se ha identificado una vulnerabilidad de tipo control de acceso inapropiado en los equipos ValveLink de Emerson que podría permitir a un atacante la ejecución arbitraria de código.

Solución:

Actualizar el dispositivo a la versión v13.4.123 o superior.

Detalle:

Una configuración insegura de los parámetros podría permitir a un atacante local, sin privilegios, llevar a cabo la escalada de privilegios. Se ha asignado el identificador CVE-2020-6971 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Consumo descontrolado de recursos en PLC CJ Series de Omron

Fecha de publicación: 04/03/2020

Importancia: Alta

Recursos afectados:

Omron PLC CJ Series, todas las versiones.

Descripción:

Jipeng You (XDU) ha identificado una vulnerabilidad, de tipo consumo descontrolado de recursos y con severidad alta, en los equipos PLC CJ Series de Omron. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante causar una denegación de servicio en el sistema afectado.

Solución:

El fabricante recomienda configurar un *firewall* para filtrar el acceso al puerto FINS (por defecto es el 9600) y las conexiones IP de los dispositivos conectados.

Detalle:

Un atacante puede enviar una serie de paquetes de datos específicos dentro de un periodo corto de tiempo, causando un error de servicio en el módulo PLC Ethernet, lo que resultaría en una denegación de servicio en el PLC. Se ha reservado el identificador CVE-2020-6986 para dicha vulnerabilidad.

Etiquetas: Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en productos TC Router y TC Cloud Client de Phoenix Contact

Fecha de publicación: 06/03/2020

Importancia: Crítica

Recursos afectados:

- TC ROUTER:
  - TC ROUTER 3002T-4G, versiones anteriores o iguales a la 2.05.3;
  - TC ROUTER 3002T-4G, versiones anteriores o iguales a la 2.05.3;
  - TC ROUTER 2002T-3G, versiones anteriores o iguales a la 2.05.3;
  - TC ROUTER 2002T-3G, versiones anteriores o iguales a la 2.05.3;
  - TC ROUTER 3002T-4G VZW, versiones anteriores o iguales a la 2.05.3;
  - TC ROUTER 3002T-4G ATT, versiones anteriores o iguales a la 2.05.3.
- TC CLOUD CLIENT:
  - TC CLOUD CLIENT 1002-4G, versiones anteriores o iguales a la 2.03.17;
  - TC CLOUD CLIENT 1002-4G VZW, versiones anteriores o iguales a la 2.03.17;
  - TC CLOUD CLIENT 1002-4G ATT, versiones anteriores o iguales a la 2.03.17;
  - TC CLOUD CLIENT 1002-TXTX, versiones anteriores o iguales a la 1.03.17.

Descripción:

Thomas Weber, de SEC Consult Vulnerability Lab, ha identificado múltiples vulnerabilidades de tipo inyección de comandos, falta de validación de nombres de archivos de entrada y uso de certificado fijo en el hardware, que podrían permitir a un atacante ejecutar código remoto, escribir archivos arbitrarios, inyectar comandos y divulgar información sensible.

Solución:

Actualizar a las siguientes versiones:

- TC ROUTER:
  - TC ROUTER 3002T-4G, 2.05.4,
  - TC ROUTER 3002T-4G, 2.05.4,
  - TC ROUTER 2002T-3G, 2.05.4,
  - TC ROUTER 2002T-3G, 2.05.4,
  - TC ROUTER 3002T-4G VZW, 2.05.4,
  - TC ROUTER 3002T-4G ATT, 2.05.4.
- TC CLOUD CLIENT:
  - TC CLOUD CLIENT 1002-4G, 2.03.18,
  - TC CLOUD CLIENT 1002-4G VZW 2.03.18,
  - TC CLOUD CLIENT 1002-4G ATT 2.03.18,
  - TC CLOUD CLIENT 1002-TXTX 1.03.18.

Detalle:

- En BusyBox 1.27.2, la función de autocompletar en la shell, usado para conseguir una lista de nombres de archivo en un directorio, no controla los nombres de archivos, por lo que permite la ejecución de cualquier secuencia escapada en el terminal. Se ha asignado el identificador CVE-2017-16544 para esta vulnerabilidad.
- El envío de una petición POST a un programa CGI, el cual está disponible en la interfaz web, podría permitir a un atacante la inyección de comandos. Se ha asignado el identificador CVE-2020-9436 para esta vulnerabilidad.
- El dispositivo contiene certificados fijos en el firmware usados para ejecutar el servicio web, lo que podría permitir la suplantación de identidad, ataques man-in-the-middle o descifrado pasivo de ataques, si el certificado genérico no es reemplazado por un certificado específico durante la instalación. Se ha asignado el identificador CVE-2020-9435 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en MicroLogix Controllers de Rockwell Automation

Fecha de publicación: 09/03/2020

Importancia: Crítica

Recursos afectados:

- MicroLogix 1400 Controllers:
  - Series B, v21.001 y anteriores;
  - Series A, todas las versiones.
- MicroLogix 1100 Controllers, todas las versiones.
- Software RSLogix 500, versiones V12.001 y anteriores.

Descripción:

Se han reportado múltiples vulnerabilidades presentes en los controladores MicroLogix y en el softeare RSLogix 500 que podrían permitir a un atacante ganar acceso a información confidencial, incluyendo contraseñas.

Solución:

Aplicar las siguientes actualizaciones disponibles:

- Para MicroLogix 1400 Controllers, Series BP, la versión FRN 21.002.
- Para el software RSLogix 500, la versión V11.

Detalle:

A continuación, se describen las vulnerabilidades críticas detectadas:

- La clave de cifrado utilizada para proteger la contraseña está embebida en el documento binario del RSLogix 500. Un atacante podría obtener la clave cifrada y realizar ataques remotos obteniendo accesos no autorizados al controlador. Se ha asignado el identificador CVE-2020-6990 para esta vulnerabilidad.
- La función de cifrado utilizada para proteger la contraseña de acceso al dispositivo puede ser descubierta por un atacante remoto, que podría obtener un acceso no autorizado al controlador. Se ha asignado el identificador CVE-2020-6984 para esta vulnerabilidad.

Para el resto de las vulnerabilidades, de severidad media, se han reservado los identificadores CVE- 2020-6988 y CVE-2020-6980.

Etiquetas: Actualización

Múltiples vulnerabilidades en productos de WAGO

Fecha de publicación: 09/03/2020

Importancia: Crítica

Recursos afectados:

- Series PFC100 750-81xx/xxx-xxx, todas las versiones de *firmware*;
- Series PFC200 750-82xx/xxx-xxx, versión de *firmware* 4 o superiores;
- Touch Panel 600 Standard Line 762-4xxx;
- Touch Panel 600 Advanced Line 762-5xxx;
- Touch Panel 600 Marine Line 762-6xxx.

Descripción:

Los investigadores Nico Jansen de FH Aechen, Carl Hurd, Kelly Leuschner, Daniel Patrick DeSantis y Lilith de Cisco Talos, Daniel Szameitat y Jan Hoff de SE han identificado múltiples vulnerabilidades en distintos productos de WAGO. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante escuchar y manipular el tráfico de red, obtener información sensible, provocar una condición de denegación de servicio, neutralización indebida de elementos especiales, validación incorrecta de entradas y dependencia del nombre o la extensión del archivo.

Solución:

- Para las vulnerabilidades CVE-2019-5106 y CVE-2019-5107 se recomienda deshabilitar el puerto TCP 11740 y el UDP 1740 o utilizar una conexión VPN cifrada al dispositivo.
- Para las vulnerabilidades CVE-2019-5134 y CVE-2019-5135 se recomienda actualizar los dispositivos a la versión 15 de *firmware* o superior.
- Para la vulnerabilidad CVE-2019-5149 se recomienda proteger el dispositivo de accesos no autorizados.
- Para las vulnerabilidades CVE-2019-5158 y CVE-2019-5159 se recomienda validar la integridad del paquete de actualización de WUP verificando el *hash* del archivo antes de iniciar la actualización de *firmware*.
- Para las vulnerabilidades CVE-2019-5155, CVE-2019-5156, CVE-2019-5157, CVE-2019-5160 y CVE-2019-5161 se recomienda utilizar contraseñas robustas para todos los usuarios, especialmente para cuentas administrativas.
- Para el resto de vulnerabilidades se recomienda deshabilitar el servicio I/O-Check después de la puesta en marcha del dispositivo.

Detalle:

- La vulnerabilidad de severidad crítica, de tipo dependencia del nombre o la extensión del archivo, permitiría a un atacante que tiene privilegios de administración en el dispositivo, redirigirse a su propia cuenta en la nube de Azure e instalar software malicioso con la funcionalidad de actualización del *firmware*. Se ha reservado el identificador CVE-2019-5161 para esta vulnerabilidad.
- Un atacante que aprovechara alguna de las vulnerabilidades restantes podría realizar alguna de las siguientes acciones:
    - descifrar la contraseña;
    - exposición de información sensible;
    - denegación de servicio;
    - inyección de comandos del sistema operativo;
    - control de accesos no controlado;
    - escritura de archivos en rutas arbitrarias;
    - instalación de *firmware* obsoleto;
    - desbordamiento de búfer;
    - ejecución de código;
    - corrupción de memoria.

Para el resto de vulnerabilidades, se han reservado los siguientes identificadores: CVE-2019-5106, CVE-2019-5107, CVE-2019-5134, CVE-2019-5135, CVE-2019-5149, CVE-2019-5155, CVE-2019-5156, CVE-2019-5157, CVE-2019-5160, CVE-2019-5158, CVE-2019-5159, CVE-2019-5166, CVE-2019-5167, CVE-2019-5168, CVE-2019-5169, CVE-2019-5170, CVE-2019-5171, CVE-2019-5172, CVE-2019-5173, CVE-2019-5174, CVE-2019-5175, CVE-2019-5176, CVE-2019-5177, CVE-2019-5178, CVE-2019-5179, CVE-2019-5180, CVE-2019-5181, CVE-2019-5182, CVE-2019-5184, CVE-2019-5185 y CVE-2019-5186.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Boletín de seguridad de Siemens de marzo de 2020

Fecha de publicación: 10/03/2020

Importancia: Alta

Recursos afectados:

- Spectrum Power™ 5, todas las versiones anteriores a 5.50 HF02;
- Familia SIMATIC S7-300 CPU (incluido las relacionadas con CPUs ET200 y variantes de SIPLUS), todas las versiones anteriores a 3.X.17;
- SINUMERIK 840D sl, todas las versiones;
- SiNVR 3 Central Control Server (CCS), todas las versiones;

- SiNVR 3 Video Server, todas las versiones.

Descripción:

Este aviso contiene 12 vulnerabilidades que afectan a múltiples productos de Siemens, de las cuales 5 son de severidad alta y 7 de severidad media.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas, pueden obtenerse desde el panel de descarga de Siemens. Para los productos sin actualizaciones disponibles, aplicar las medidas de mitigación descritas en la sección de *Referencias*.

Detalle:

Un atacante que aproveche alguna de las vulnerabilidades de severidad alta descritas en este aviso, podría realizar alguna de las siguientes acciones:

- ejecución de operaciones en la base de datos a través de una inyección SQL;
- ejecución de comandos del sistema operativo;
- acceso y descarga de archivos arbitrarios del servidor;
- denegación de servicio;
- obtención de contraseñas;
- hacer que el dispositivo afectado pase a modo por defecto.

Se han reservado los siguientes identificadores para estas vulnerabilidades: CVE-2019-19290, CVE-2019-19296, CVE-2019-19297, CVE-2019-19291, CVE-2019-19299, CVE-2019-19292, CVE-2019-19293, CVE-2019-19294, CVE-2019-19295, CVE-2019-19298, CVE-2019-18336 y CVE-2020-7579.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en productos de Johnson Controls

Fecha de publicación: 11/03/2020

Importancia: Crítica

Recursos afectados:

- Kantech EntraPass Corporate Edition, versión 8.10 y anteriores;
- Kantech EntraPass Global Edition, versión 8.10 y anteriores;
- Metasys Application and Data Server, versión 10.1 y anteriores;
- Metasys Extended Application and Data Server, versión 10.1 y anteriores;
- Metasys Open Data Server, versión 10.1 y anteriores;
- Metasys Open Application Server, versión 10.1 y anteriores;
- Metasys Network Automation Engine, versiones 9.0.1, 9.0.2, 9.0.3, 9.0.5 y 9.0.6;
- Metasys Network Integration Engine, versiones 9.0.1, 9.0.2, 9.0.3, 9.0.5 y 9.0.6;
- Metasys NAE85 y NIE85, versión 10.1 y anteriores;
- Metasys LonWorks Control Server, versión 10.1 y anteriores;
- Metasys System Configuration Tool, versión 13.2 y anteriores;
- Metasys Smoke Control Network Automation Engine, versión 8.1.

Descripción:

Se han reportado vulnerabilidades que afectan a múltiples productos de Johnson Controls y que podrían permitir a un atacante ejecutar código malicioso con privilegios del sistema, provocar un ataque de denegación de servicio o acceder a información sensible.

Solución:

Actualizar a la versión 8.10 de EntraPass.

Detalle:

- Un problema en la API podría permitir a un atacante remoto subir y ejecutar código malicioso con privilegios del sistema. Se ha asignado el identificador CVE-2019-7589 para esta vulnerabilidad.
- Una vulnerabilidad XXE podría permitir a un atacante extraer archivos ASCII del servidor. Se ha asignado el identificador CVE-2020-9044 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Manipulación del arranque seguro en Stratix 5950 de Rockwell Automation

Fecha de publicación: 11/03/2020

Importancia: Media

Recursos afectados:

- Stratix 5950 1783-SAD4T0SBK9;
- Stratix 5950 1783-SAD4T0SPK9;
- Stratix 5950 1783-SAD2T2SBK9;
- Stratix 5950 1783-SAD2T2SPK9.

Descripción:

Una vulnerabilidad de Cisco de criticidad media afecta al producto Stratix 5950 de Rockwell Automation. Un atacante local, autenticado, podría instalar y arrancar una imagen de software malicioso.

Solución:

Rockwell Automation recomienda aplicar la actualización FRN v6.4.0.

Detalle:

Una vulnerabilidad en la lógica que maneja el control de acceso a uno de los componentes de hardware en la implementación del arranque seguro de Cisco podría permitir a un atacante local, autenticado, instalar y arrancar una imagen de software malicioso. Se ha asignado el identificador CVE-2019-1649 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Denegación de servicio en acopladores BK9000 de Beckhoff Automation

Fecha de publicación: 11/03/2020

Importancia: Alta

Recursos afectados:

BK9000 Ethernet TCP/IP Bus Coupler, en todas sus versiones.

Descripción:

El investigador Martin Menschner, de Rhebo GmbH, ha reportado a Beckhoff Automation, una vulnerabilidad de tipo consumo de recursos no controlado que afecta al dispositivo BK9000. El fabricante, a su vez, ha notificado esta vulnerabilidad al Un atacante remoto podría generar una condición de denegación de servicio en los acopladores.

Solución:

Los clientes deben configurar un firewall perimetral para bloquear el tráfico desde redes no confiables o seguras hacia el dispositivo.

Detalle:

La función del acoplador podría verse suspendida por un ataque de denegación de servicio. El acoplador no se recuperará después de que el ataque se haya detenido. Un reinicio del dispositivo recuperaría la operación. Se ha reservado el identificador CVE-2020-9464 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Schneider Electric

Fecha de publicación: 12/03/2020

Importancia: Alta

Recursos afectados:

- IGSS que utilicen el servicio IGSSupdate, versión 14 y anteriores;
- Módulo Quantum Ethernet Network 140NOE771x1, version 7.0 y anteriores;
- Procesadores Quantum 140CPU65xxxxx con Ethernet integrado, todas las versiones;
- Procesadores Premium con Ethernet integrado, todas las versiones;
- Kit de instalación de ZigBee, todas las versiones anteriores a la 1.0.1;
- Andover Continuum Controllers, todas las versiones.

Descripción:

Los investigadores Yongjun Liu, de Nsfocus, Trend Micro Zero Day Inititative, el CNITSEC, y el investigador, Niv Levy, han reportado siete vulnerabilidades: cuatro de criticidad alta y tres medias, que afectan a diversos productos de Schneider Electric. Un atacante podría realizar escaladas de privilegios, generar una condición de denegación de servicio, ejecución de código malicioso o acceso a información sin la autenticación necesaria.

Solución:

Schneider Electric ha publicado varias actualizaciones para solucionar las vulnerabilidades en los productos afectados.

- ZigBee Toolkit, actualizar a la versión 1.01;
- IGSS, actualizar al la versión 14.0.0.20009;
- Módulo Quantum Ethernet Network 140NOE771x1, actualizar a la versión 7.1:
  - 140NOE77101;
  - 140NOE77111.
- Procesadores Quantum 140CPU65xxxxx con Ethernet integrado: configurar la característica ACL contempladas en el manual de usuario;
- Procesadores Premium con Ethernet integrado: configurar la característica ACL contempladas en el manual de usuario;
- Andover Continuum Controllers: se trata de un producto que se encuentra sin soporte, Schneider Electric recomienda su uso en segmentos de red aislados junto a la utilización de un firewall con ACL, inspección profunda de paquetes y filtrado de paquetes.

Detalle:

Las vulnerabilidades de criticidad altas:

- Un atacante remoto, no autenticado, podría realizar la lectura de ficheros de forma arbitraria del servidor IGSS en una red no restringida o compartida cuando el servicio de IGSS Update está activo. Se ha reservado el identificador CVE-2020-7478 para esta vulnerabilidad.
- Un atacante local podría ejecutar procesos que de otro modo requerirían una escalada de privilegios cuando se envían los comandos de red al servicio IGSS Update. Se ha reservado el identificador CVE-2020-7479 para esta vulnerabilidad.
- Un atacante remoto podría generar una condición de denegación de servicio cuando se envían comandos elaborados a través de Modbus. Se ha reservado el identificador CVE-2020-7477 para esta vulnerabilidad.
- Un atacante remoto podría interferir en el procesamiento de datos XML de una aplicación en el servidor y obtener información de los mismos. Se ha reservado el identificador CVE-2020-7480 para esta vulnerabilidad.

A las vulnerabilidades de criticidad media se les han reservado los identificadores: CVE-2020-7476, CVE-2020-7481 y CVE-2020-7482.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Múltiples vulnerabilidades en OnCell Central Manager de Moxa

Fecha de publicación: 16/03/2020

Importancia: Alta

Recursos afectados:

- OnCell Central Manager, versiones anteriores a la 2.4.1

Descripción:

El investigador, Sergey Temnikov, de Kaspersky ICS CERT, ha reportado dos vulnerabilidades de tipo revelación de información y deserialización de datos no confiables en el producto OnCell Central Manager de Moxa.

Solución:

La librería, que utiliza OnCell Central Manager, ha sido migrada a la última versión de Apache 4.7.3, para solucionar las vulnerabilidades. Se debe contactar con el fabricante para aplicar el parche de seguridad.

Detalle:

- La deserialización de datos no confiables podría permitir a un atacante la ejecución de código en el componente de terceros Apache Flex BlazeDS. Se ha asignado el identificador CVE-2019-15696 para esta vulnerabilidad.
- El procesamiento de entidades externas XML (XXE) en el componente de terceros Apache Flex BlazeDS podría permitir a un atacante la divulgación de información. Se ha asignado el identificador CVE-2019-15696 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en CNCSoft ScreenEditor de Delta Electronics

Fecha de publicación: 18/03/2020

Importancia: Alta

Recursos afectados:

- CNCSoft ScreenEditor, versiones v1.00.96 y anteriores.

Descripción:

Se han reportado varias vulnerabilidades en el producto CNCSoft ScreenEditor de Delta Electronic que podrían permitir a un atacante la divulgación de información, la ejecución remota de código o el bloqueo de la aplicación.

Solución:

Actualizar a la última versión.

Detalle:

- Un atacante podría provocar un desbordamiento de búfer mediante el envío de un fichero malicioso especialmente diseñado, cuando este es abierto por un usuario legítimo. Se ha reservado el identificador CVE-2020-7002 para esta vulnerabilidad.
- La falta de validación de los ficheros de entrada podría permitir a un atacante provocar un desbordamiento de lectura del búfer fuera de límites mediante el envio de un fichero malicioso especialmente diseñado que sea abierto por un usuario legítimo. Se ha reservado el identificador CVE-2020-6976 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Ejecución de código arbitrario en UPS Companion Software de Eaton

Fecha de publicación: 20/03/2020

Importancia: Alta

Recursos afectados:

UPS Companion Software, versiones 1.05 y anteriores.

Descripción:

El investigador, Ravjot Singh Samra, ha reportado una vulnerabilidad de criticidad alta. Un atacante adyacente podría realizar una ejecución de código arbitrario.

Solución:

El fabricante recomienda actualizar a la versión 1.06.

Detalle:

El software afectado, no neutraliza o neutraliza incorrectamente la sintaxis del código antes de usar la entrada en una llamada de evaluación dinámica. Un atacante adyacente podría ejecutar código arbitrario en la maquina en la que el software está instalado. Se ha reservado el identificador CVE-2020-6650 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en el servidor NDS-5000 de Systech Corporation

Fecha de publicación: 20/03/2020

Importancia: Media

Recursos afectados:

NDS-5000 Terminal Server, NDS/5008 (Puerto 8, RJ45), versión del firmware 02D.30.

Descripción:

El investigador, Murat Aydemir de Biznet Bilisim, ha reportado una vulnerabilidad de criticidad media. Un atacante remoto podría revelar información, limitar la disponibilidad del sistema y ejecutar código remoto.

Solución:

Systech ha publicado el fimrware (02F.6) que mitiga la vulnerabilidad.

Detalle:

El producto contiene una vulnerabilidad de tipo *Cross-site Scripting* (XSS) almacenado, lo que podría permitir a un atacante remoto realizar operaciones con privilegios de usuario, acceder a información sensible y ejecutar código en remoto. Se ha asignado el identificador CVE-2020-7006 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Control de acceso incorrecto en Omnipod Insulin Management System de Insulet

Fecha de publicación: 20/03/2020

Importancia: Alta

Recursos afectados:

Las siguientes versiones del Omnipod Insulin Management System, de Insulet, están afectadas:

- Product ID/Reorder, números 19191 y 40160;
- UDI/Model/NDC, números ZXP425 (10-Pack) y ZXR425 (10-Pack Canada).

Descripción:

La organización Thirdwayv Inc. ha reportado una vulnerabilidad de tipo control de acceso incorrecto. Esta vulnerabilidad podría permitir a un atacante acceder al producto e interceptar, modificar o interferir en la comunicación inalámbrica RF hacia o desde el producto.

Solución:

El fabricante recomienda a los usuarios afectados que contacten con su proveedor para conocer el riesgo de continuar con su uso o poder cambiar al último modelo, que cuenta con mejoras en ciberseguridad. El fabricante también ha publicado información adicional acerca de esta vulnerabilidad.

Detalle:

El protocolo de comunicación del producto afectado no implementa autorización o autenticación. Esta vulnerabilidad podría permitir acceder a información sensible, cambiar la configuración de la bomba de insulina o controlar la administración de insulina. Se ha reservado el identificador CVE-2020-10597 para esta vulnerabilidad.

Etiquetas: Actualización, Sanidad, Vulnerabilidad

Inyección de código en productos de Schneider

Fecha de publicación: 23/03/2020

Importancia: Alta

Recursos afectados:

- EcoStruxure™ Control Expert, todas las versiones anteriores a la 14.1 Hot Fix;
- Unity Pro, todas las versiones;
- Modicon M340, todas las versiones anteriores a V3.20;
- Modicon M580, todas las versiones anteriores a V3.10.

Descripción:

El investigador, Flavian Dola, de Airbus Cybersecurity, ha reportado una vulnerabilidad de tipo neutralización impropia de elementos especiales de salida usados por un componente descendente que podría permitir a un atacante remoto la transferencia de código malicioso al controlador.

Solución:

El fabricante ha lanzado un hotfix disponible para su descarga. Consulte la sección de referencias para actualizar el controlador afectado.

Detalle:

Una vulnerabilidad de tipo neutralización impropia de elementos especiales de salida usados por un componente descendente en una DLL del controlador podría permitir a un atacante remoto la transferencia de código malicioso al controlador. Se ha reservado el identificador CVE-2020-7475 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en equipamiento VBASE de VISAM

Fecha de publicación: 25/03/2020

Importancia: Crítica

Recursos afectados:

- VBASE Editor, versión 11.5.0.2;
- VBASE Web-Remote Module.

Descripción:

El investigador Gjoko Krstic, de Applied Risk, ha reportado múltiples vulnerabilidades en VBASE, del tipo: salto de ruta relativa, permisos por defecto incorrectos, fuerza de encriptación inadecuada, almacenamiento inseguro de información sensible y desbordamiento de búfer basado en pila. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante leer el contenido de archivos arbitrarios, escalar privilegios a nivel de sistema, ejecutar código arbitrario, saltarse los mecanismos de seguridad o descubrir la clave criptográfica del login web.

Solución:

Por el momento no existe un parche para estas vulnerabilidades.

Detalle:

- La entrada suministrada en la URL no es validada correctamente antes de su uso, lo que podría permitir a un atacante leer archivos arbitrarios de los recursos locales. Se ha asignado el identificador CVE-2020-7008 para esta vulnerabilidad.
- El uso de permisos de forma insegura puede permitir a un atacante la escalada de privilegios. Se ha asignado el identificador CVE-2020-7004 para esta vulnerabilidad.
- El uso de un algoritmo de hashing inseguro y débil puede permitir a un atacante saltarse el mecanismo de seguridad de acceso mediante el uso de ataques por fuerza bruta, técnicas de *crackeo* de contraseñas o sobreescritura del *hash*. Se ha asignado el identificador CVE-2020-10601 para esta vulnerabilidad.
- Un atacante, no autenticado, podría descubrir la clave criptográfica del servidor web y obtener información sobre el login en el mecanismo de encriptación, lo que podría resultar en un salto de autenticación del interfaz web HTML5 del HMI. Se ha asignado el identificador CVE-2020-7000 para esta vulnerabilidad.
- Un componente ActiveX vulnerable podría ser explotado, resultando en un desbordamiento de búfer, lo que podría permitir a un atacante remoto causar una denegación de servicio y la ejecución de código remoto. Se ha asignado el identificador CVE-2020-10599 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Credenciales insuficientemente protegidas en comunicaciones de clientes .NET y Java en OPC UA

Fecha de publicación: 25/03/2020

Importancia: Alta

Recursos afectados:

- UA .NET Standard Stack y Sample Code,
- UA .NET Legacy Stack y Sample Code,
- UA Java Legacy Stack.

Descripción:

El investigador Bernd Edlinger, de Softing, ha detectado una vulnerabilidad de criticidad alta que afecta a los clientes OPC .NET y Java. Un atacante remoto podría obtener las credenciales y reutilizarlas.

Solución:

- UA .NET Standard Stack y Sample Code, aplicar el parche de seguridad o actualizar NuGet Packages a la versión 1.4.359.31;
- UA .NET Legacy Stack y Sample Code, aplicar el parche de seguridad;
- UA Java Legacy Stack, aplicar el parche de seguridad.

Detalle:

Los clientes OPC UA basados en .NET y Java contienen una vulnerabilidad que podría permitir un atacante remoto interceptar las comunicaciones mediante un ataque del tipo *man in the middle*, obtener las credenciales cifradas enviadas y reutilizarlas. Se ha asignado el identificador CVE-2019-19135 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos de Codesys V3

Fecha de publicación: 26/03/2020

Importancia: Crítica

Recursos afectados:

Todas las variantes de los siguientes productos CODESYS V3 en todas las versiones anteriores a V3.5.15.40 que contengan los componentes CmpRouter, CmpRouterEmbedded, CmpWevServer o CmpWebServerHandler:

- CODESYS Control para BeagleBone,
- CODESYS Control para emPC-A/iMX6,
- CODESYS Control para IOT2000,
- CODESYS Control para Linux,
- CODESYS Control para PLCnext,
- 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 CODESYS Development System setup),
- CODESYS Control V3 Runtime System Toolkit,
- CODESYS V3 Embedded Target Visu Toolkit,
- CODESYS V3 Remote Target Visu Toolkit,
- CODESYS V3 Safety SIL2,
- CODESYS Edge Gateway V3,
- CODESYS Gateway V3,
- CODESYS HMI V3,
- CODESYS OPC Server V3,
- CODESYS PLCHandler SDK,
- CODESYS Control para BeagleBone,
- CODESYS V3 Simulation Runtime (parte de CODESYS Development System).

Descripción:

El investigador Carl Hurd, de Cisco Talos, un cliente OEM y Tenable han reportado dos vulnerabilidades, una de severidad crítica y otra alta, que afectan a equipamiento de Codesys V3. Un atacante remoto podría generar una denegación de servicio o la ejecución de código arbitrario.

Solución:

3S-Smart Software Solutions GmbH ha publicado la versión V3.5.15.40 que soluciona dichas vulnerabilidades.

Detalle:

- La vulnerabilidad de severidad crítica se debe a que el servidor web de Codesys es utilizado por WebVisu para mostrar pantallas de visualización en el navegador web. Peticiones especialmente creadas podrían causar un desbordamiento de búfer basado en memoria dinámica (*heap*), lo que podría resultar en un bloqueo en el navegador, pudiendo originar una condición de denegación de servicio o ejecutar código remoto. Se ha asignado el identificador CVE-2020-10245 para esta vulnerabilidad.
- La vulnerabilidad de severidad alta se debe a que los productos de Codesys mencionados soportan un protocolo de *routing* para la comunicación entre clientes y el Codesys Control *runtime*. Paquetes de comunicación especialmente creados pueden desencadenar una lectura de búfer fuera de límites en la pila de comunicación, lo que podría generar una condición de denegación de servicio. Se ha asignado el identificador CVE-2019-5105 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de desbordamiento de búfer en WebAccess de Advantech

Fecha de publicación: 27/03/2020

Importancia: Alta

Recursos afectados:

WebAccess, versión 8.4.2 y anteriores.

Descripción:

Peter Cheng, de Elex CyberSecurity, Inc., ha reportado una vulnerabilidad clasificada de severidad alta, de desbordamiento de búfer al CISA.

Solución:

Actualizar WebAccess a la versión 8.4.4.

Detalle:

Una vulnerabilidad de desbordamiento de búfer basada en pila (*stack*), causada por la falta de validación adecuada de la longitud de los datos suministrados por el usuario, podría permitir la ejecución remota del código. Se ha reservado el identificador CVE-2020-10607 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en productos de Phoenix Contact

Fecha de publicación: 27/03/2020

Importancia: Alta

Recursos afectados:

- PORTICO SERVER 1 CLIENT, versión 3.0.7 y anteriores;
- PORTICO SERVER 4 CLIENT, versión 3.0.7 y anteriores;
- PORTICO SERVER 16 CLIENT, versión 3.0.7 y anteriores;
- PC WORX SRT 2701680, versión 1.14 y anteriores.

Descripción:

Sharon Brizinov, de ClarotyCarl, y otro investigador anónimo, han reportado dos vulnerabilidades de criticidad alta que afectan a equipamiento de Phoenix Contact. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante local la ejecución de código malicioso con permisos de sistema u obtener permisos de administrador en el dispositivo.

Solución:

- Actualizar los dispositivos PORTICO a la versión V3.0.8 o superior.
- Para los dispositivos PC WORX SRT, Phoenix Contact recomienda el uso del software en sistemas con usuario único.

Detalle:

- Si el software se ejecuta como un servicio, un usuario con acceso limitado puede obtener privilegios de administrador mediante la ejecución de una consola con permisos de administrador desde el dialogo 'Importar/Exportar' en la configuración. Se ha reservado el identificador CVE-2020-10940 para esta vulnerabilidad.
- Si la aplicación PC WORX SRT está instalada como servicio, la ruta de instalación de la aplicación está configurada con permisos inseguros, lo que podría permitir a un usuario sin privilegios la escritura de archivos aleatoria en el directorio de instalación donde están localizados todos los archivos y binarios del servicio. Se ha reservado el identificador CVE-2020-10939 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de escalada de privilegios locales en GE Digital CIMPLICITY

Fecha de publicación: 31/03/2020

Importancia: Media

Recursos afectados:

GE Digital CIMPLICITY, versión 10 y anteriores.

Descripción:

Investigadores de Claroty han descubierto que GE Digital CIMPLICITY HMI/SCADA es vulnerable a una escalada de privilegios locales.

Solución:

Actualizar el producto afectado a la versión 11.0, poniéndose en contacto con el representante local de la empresa.

Detalle:

Un atacante, con acceso al sistema a través de una cuenta autenticada, podría modificar el sistema del cliente y realizar una ejecución arbitraria de código en un contexto de privilegios elevados. El atacante solo puede aprovechar esta vulnerabilidad si tiene acceso a una sesión autenticada, y existen directorios en la variable de entorno *PATH* que son modificables por la cuenta a la que el atacante tiene

acceso.

Etiquetas: Actualización, SCADA, Vulnerabilidad

Consumo incontrolado de recursos en múltiples productos de Mitsubishi Electric

Fecha de publicación: 31/03/2020

Importancia: Alta

Recursos afectados:

Todas las versiones de MELSEC iQ-R, iQ-F?Q?L y la serie de controladores programables F con puerto de transmisión MELSOFT en el puerto Ethernet.

Descripción:

Rongkuan Ma, Jie Meng y Peng Cheng han reportado una vulnerabilidad del tipo consumo incontrolado de recursos que afecta a múltiples productos de Mitsubishi Electric y que podría permitir a un atacante bloquear el puerto de transmisión MELSOFT (UDP/IP), haciendo que su estado entre en una condición no procesable.

Solución:

Mitsubishi Electric no ha liberado ninguna actualización para solucionar dicha vulnerabilidad, pero recomienda a los clientes utilizar un cortafuegos para evitar accesos remotos al dispositivo.

Detalle:

Cuando el puerto de transmisión MELSOFT entra en una condición no procesable, los clientes autorizados no pueden conectarse a él y los dispositivos que se comuniquen en otros puertos de transmisión serán dificilmente accesibles. Además, esta vulnerabilidad no afectará a otras funciones que no sean la comunicación Ethernet. No se ha asignado ningún identificador para esta vulnerabilidad.

Etiquetas: Vulnerabilidad