Boletín de abril de 2020

Avisos de Sistemas de Control Industrial

Desbordamiento de búfer en múltiples productos de Hirschmann

Fecha de publicación: 01/04/2020

Importancia: Crítica

Recursos afectados:

- Los dispositivos RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED que emplean HiOS en la versión 07.0.02 y anteriores.
- Los dispositivos EAGLE20/30, que emplean HiSecOS en la versión 03.2.00 y anteriores.

Descripción:

Los investigadores Sebastian Krause y Toralf Gimpel, de GAI NetConsult GmbH, han reportado una vulnerabilidad de severidad crítica que afecta a múltiples productos de Hirschmann. Un atacante remoto, no autenticado, podría realizar un desbordamiento de búfer y comprometer el dispositivo.

Solución:

- Actualizar los productos que utilizan HiOS a la versión 07.0.03 o superior.
- Actualizar los productos que utilizan HiSecOS a la versión 03.3.00 o superior.

Detalle:

La vulnerabilidad se debe a un análisis inapropiado de los argumentos del URL. Un atacante podría explotar esta vulnerabilidad creando específicamente solicitudes HTTP para desbordar un búfer interno. Se ha reservado el identificador CVE-2020-6994 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de fuga de información en Tab-Ex 02 de PEPPERL FUCHS

Fecha de publicación: 01/04/2020

Importancia: Baja

Recursos afectados:

Tab-Ex 02, versión 01.03.2020 y anteriores.

Descripción:

Investigadores de ESET han reportado una vulnerabilidad, de severidad baja, conocida como *Kr00k*, de tipo fuga de información, que afecta al producto Tab-Ex 02 del fabricante PEPPERL FUCHS.

Solución:

El fabricante planea publicar una actualización en mayo de 2020 para el producto afectado.

Detalle:

La vulnerabilidad detectada afecta al tráfico cifrado de wifi para los dispositivos que utilizan los chipsets Broadcom o Cypress, permitiendo

a un atacante descifrar parte del tráfico WPA2-Personal/Enterprise, forzando a un AP(*Access Point*)/cliente a empezar a utilizar una clave de cifrado *all-zero.* Se ha asignado el identificador CVE-2019-15126 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Vulnerabilidad

Vulnerabilidad de escape del entorno de escritorio restringido en productos de Becton, Dickinson and Company (BD)

Fecha de publicación: 01/04/2020

Importancia: Media

Recursos afectados:

- Pyxis MedStation ES System, versión 1.6.1;
- Pyxis Anesthesia (PAS) ES System, versión 1.6.1.

Descripción:

El equipo de BD ha reportado una vulnerabilidad de fallo del mecanismo de protección en múltiples productos de BD que podría permitir a un atacante con acceso físico ver y/o modificar datos sensibles del dispositivo.

Solución:

BD no ha liberado ninguna actualización para solucionar dicha vulnerabilidad, pero recomienda a los clientes aplicar las siguientes medidas:

- Limitar el acceso físico a los sistemas Pyxis Medstation ES y Anesthesia (PAS) ES sólo a los usuarios autorizados;
- aislar los sistemas impactados y conéctelos sólo a los sistemas de confianza;
- vigilar e investigar los reinicios imprevistos de los sistemas utilizando las herramientas de vigilancia de redes proporcionadas por los departamentos de TI.

Detalle:

Una vulnerabilidad de escape del entorno de escritorio restringido, en la funcionalidad del modo quiosco de los dispositivos afectados, podría permitir a un atacante acceder a datos sensibles mediante entradas especialmente diseñadas. Se ha asignado el identificador CVE-2020-10598 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de ABB

Fecha de publicación: 03/04/2020

Importancia: Crítica

Recursos afectados:

- System 800xA Base, versión 6.1 y anteriores;
- System 800xA Information Manager:
  - versión 5.1;
  - versión 6.0.0, hasta la 6.0.3.2;
  - versión 6.1.
- TG/S 3.2 Telephone Gateway, Analogue, MDRC;
- 6186/11 Telefon-Gateway, Analog (Busch-Jaeger brand);
- OPC Server para AC800M, versión 6.0 y anteriores;
- Control Builder MProfessional, versión 6.1 y anteriores;
- MMSServer para AC800M, versión 6.1 y anteriores;
- Base Software para SoftControl, versión 6.1 y anteriores;

Descripción:

Los investigadores, William Knowles, de Applied Risk, y Maxim Rupp, han reportado 8 vulnerabilidades, dos de severidad crítica, tres altas y tres medias, que afectan a múltiples productos de ABB. Un atacante, con acceso remoto, podría provocar la detención del dispositivo, la ejecución de código de forma arbitraria, tomar el control del dispositivo y realizar una escalada de privilegios.

Solución:

- System 800xA Base, puede solucionarse mediante cualquiera de las siguientes acciones:
  - actualizar a la última versión 6.1 disponible;
  - actualizar a la versión 6.0.3 LTS, después de la 6.0.33.
- TG/S 3.2 Telephone Gateway, Analogue, MDR y 6186/11 Telefon-Gateway, Analog (Busch-Jaeger brand):
  - Configurar los dispositivos, únicamente, en redes seguras.
- Actualizar a la versión 6.0.3 LTS, después de la 6.0.3.3:
  - System 800xA Information Manager,
  - MMSServer para AC800M,
  - OPC Server para AC800M,
  - Control Builder MProfessional,
  - Base Software para SoftControl.

Detalle:

A continuación se detallan las vulnerabilidades con severidades críticas y altas:

- La configuración de control de acceso para el registro de Windows permite a los usuarios con pocos privilegios leer y modificar el contenido utilizado por las funciones del sistema. Un atacante autenticado podría causar el mal funcionamiento de diferentes sistemas. Se ha reservado el identificador CVE-2020-8474 para esta vulnerabilidad.
- Un componente vulnerable en el servidor de mensajería instantánea (IM) podría permitir a un atacante ejecutar código arbitrario en el equipo de la víctima. Para explotar con éxito esta vulnerabilidad, es necesario persuadir al usuario para que acceda a un sitio web malicioso. Se ha reservado el identificador CVE-2020-8477 para esta vulnerabilidad.
- Al acceder a una *URL* específica en el servidor web integrado del producto, un usuario malicioso podría acceder a diferentes puntos finales de la aplicación sin autenticarse, evadiendo las normas de control de acceso (ACL). Un atacante podría obtener información confidencial o la escalada de privilegios. Se ha reservado el identificador CVE-2019-19104 para esta vulnerabilidad.
- La aplicación no emplea reglas adecuadas de control de acceso (ACL). Un atacante podría obtener información o modificar las configuraciones del sistema. Se ha reservado el identificador CVE-2019-19106 para esta vulnerabilidad.
- Un atacante que explotara con éxito la vulnerabilidad en una de las funciones de la Base 800xA del Sistema ABB podría realizar una escalada de privilegios, ejecutar un código arbitrario y afectar a varias funciones de ingeniería, lo que conduciría a aplicaciones corruptas. Se ha asignado el identificador CVE-2020-8473 para esta vulnerabilidad.

Al resto de las vulnerabilidades se les han asignado los identificadores: CVE-2019-19105, CVE-2019-19107 y CVE-2020-8472.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en Automation Studio de B&R

Fecha de publicación: 03/04/2020

Importancia: Alta

Recursos afectados:

Automation Studio, versiones:

- 4.0.x;
- 4.1.x;
- 4.2.x;
- 4.3.11SP y anteriores;
- 4.4.9SP y anteriores;
- 4.5.4SP y anteriores;
- 4.6.3SP y anteriores;
- 4.7.2 y anteriores;
- 4.8.1 y anteriores.

Descripción:

El investigador, Nadav Erez, ha reportado tres vulnerabilidades de tipo gestión de privilegios incorrecta, limitación incorrecta de nombre de ruta a un directorio restringido y falta del paso de cifrado requerido que podrían permitir a un atacante eliminar archivos arbitrariamente, buscar archivos arbitrarios o realizar operaciones de escritura arbitrarias en el producto Automation Studio.

Solución:

Actualizar a la última versión.

Detalle:

- Una escalada de privilegios en el servicio de actualización de B&R Automation Studio podría permitir a atacante autenticado borrar archivos arbitrarios a través de una interfaz expuesta. Se ha reservado el identificador CVE-2019-19100 para esta vulnerabilidad.
- Una comunicación con falta de seguridad y una validación incompleta TLS en el servicio de actualización, podrían permitir a un atacante no autenticado realizar ataques MITM a través del servicio de actualización B&R. Se ha reservado el identificador CVE-2019-19101 para esta vulnerabilidad.
- Una vulnerabilidad transversal del directorio en SharpZipLib es utilizada en el servicio de actualización en B&R lo que podría permitir a un atacante no autenticado escribir en ciertos directorios locales. Se ha reservado el identificador CVE-2019-19102 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Advantech WebAccess/NMS

Fecha de publicación: 08/04/2020

Importancia: Crítica

Recursos afectados:

WebAccess/NMS, versiones anteriores a 3.0.2.

Descripción:

rgod, de 9sg, trabajando con Zero Day Initiative de Trend Micro, ha reportado 8 vulnerabilidades, siendo 2 de severidad crítica, 5 altas y 1 media. Los tipos de vulnerabilidades son: subida de ficheros potencialmente maliciosos sin restricción, inyección SQL, acceso relativo a rutas no controlado (*relative path traversal*), falta de autenticación para función crítica, restricción impropia de referencias a XXE (*XML eXternal Entities*) e inyección de comandos del SSOO.

Solución:

Actualizar el producto afectado a la versión 3.0.2.

Detalle:

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

- subir archivos potencialmente maliciosos y ejecutarlos;
- acceder a información sensible;
- eliminar o modificar ficheros fuera del control de la aplicación;
- crear perfiles de administrador;
- ejecutar comandos del sistema de manera remota.

Se han reservado los siguientes identificadores para estas vulnerabilidades: CVE-2020-10617, CVE-2020-10623, CVE-2020-10619, CVE-2020-10631, CVE-2020-10625, CVE-2020-10629 y CVE-2020-10603.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad en Fuji Electric V-Server Lite

Fecha de publicación: 08/04/2020

Importancia: Alta

Recursos afectados:

V-Server Lite, todas las versiones anteriores a la 4.0.9.0.

Descripción:

Una vulnerabilidad de desbordamiento de búfer basado en memoria dinámica (*heap*) podría permitir a un atacante remoto la ejecución remota de código.

Solución:

Actualizar a la versión 4.0.9.0.

Detalle:

El búfer asignado a la lectura de datos, al analizar los archivos VPR, es demasiado pequeño, lo que podría permitir a un atacante remoto escalar privilegios para la ejecución remota de código. Se ha reservado el identificador CVE-2020-10646 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad en la integridad de las comunicaciones en KUKA Sim Pro

Fecha de publicación: 08/04/2020

Importancia: Media

Recursos afectados:

KUKA Sim Pro, versión 3.1 del *software* de simulación y programación de máquinas.

Descripción:

Federico Maggi, de Trend Micro, ha reportado al CISA una vulnerabilidad en KUKA Sim Pro, de severidad media, de aplicación incorrecta de la integridad de los mensajes durante transmisiones en un canal de comunicación.

Solución:

Actualizar el producto afectado a la versión 3.1.2.

Detalle:

Esta vulnerabilidad podría provocar una pérdida de integridad en los modelos 3D externos obtenidos de servidores remotos. Cuando estos dispositivos solicitan un modelo, el servidor transmite el modelo en texto plano. Se ha reservado el identificador CVE-2020-10635 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Universal Robots

Fecha de publicación: 08/04/2020

Importancia: Crítica

Recursos afectados:

- UR10,
- UR5,
- UR 3,

- Universal Robots Robot Controllers CB 2, CB3 y e-series.

Descripción:

Investigadores de Alias Robotics, en colaboración con investigadores independientes, han detectado 86 vulnerabilidades, 29 con severidades críticas, 37 altas, 19 medias y 1 baja.

De las vulnerabilidades mencionadas, caben destacar dos de severidad crítica (CVE-2020-10264 y CVE-2020-10265), y dos altas (CVE-2020-10266 y CVE-2020-10267).

Solución:

Actualmente no hay actualizaciones que solucionen las vulnerabilidades.

Para la vulnerabilidad con identificador CVE-2020-10266, se recomienda emplear como medida de mitigación, firmar digitalmente los componentes de la plataforma UR , y validar la firma durante el proceso de instalación.

Para la vulnerabilidad con identificador CVE-2020-10267 se recomienda emplear como medida de mitigación, usar una combinación de cifrado y firma para proteger las propiedades intelectuales instaladas. Asegurar que el sistema de archivos donde residen estos ficheros tengan permisos de solo lectura, excepto para modificaciones autorizadas.

Este aviso se actualizará según se publiquen nuevas actualizaciones.

Detalle:

Las vulnerabilidades podrían permitir a un atacante realizar alguna de las siguientes acciones:

- Revelar información sensible.
- Obtener el control del sistema de manera remota.
- Realizar modificaciones en el sistema.
- Ejecución remota de código.
- Generar una condición de denegación de servicio.
- Cierre inesperado del sistema.

Etiquetas: Vulnerabilidad

Asignación incorrecta de permisos en RSLinx Classic de Rockwell Automation

Fecha de publicación: 13/04/2020

Importancia: Alta

Recursos afectados:

RSLinx Classic, versión 4.11.00 y anteriores.

Descripción:

Investigadores de Applied Risk reportaron una vulnerabilidad al fabricante, de severidad alta, y de tipo asignación de permisos incorrecta para recursos críticos.

Solución:

Aplicar el parche 1091155 para versiones desde 3.60 hasta 4.11, aunque el fabricante recomienda actualizar el producto afectado a la versión más reciente.

Detalle:

Un atacante local, autenticado, podría aprovechar esta vulnerabilidad para modificar una clave de registro, lo que conduciría a la ejecución de código malicioso utilizando los privilegios del sistema al abrir RSLinx Classic. Se ha reservado el identificador CVE-2020-10642 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Boletín de seguridad de Siemens de abril de 2020

Fecha de publicación: 14/04/2020

Importancia: Crítica

Recursos afectados:

- Climatix POL908 (BACnet/IP module), todas las versiones;
- Climatix POL909 (AWM module), todas las versiones;
- IE/PB-Link V3, todas las versiones;
- KTK ATE530S, todas las versiones;
- RUGGEDCOM RM1224, todas las versiones anteriores a la versión 6.1;
- RUGGEDCOM ROX II, todas las versiones anteriores a la versión 2.13.3;
- SCALANCE:
  - M-800 family, todas las versiones anteriores a la versión 6.1;
  - S615, todas las versiones anteriores a la versión 6.1;
  - SC-600, todas las versiones anteriores a la versión 2.0;
  - W1700 IEEE 802.11ac, todas las versiones anteriores a la versión 2.0;
  - W700 IEEE 802.11a/b/g/n, todas las versiones anteriores a la versión 6.4;
  - X-200 switch family (incluidas las variantes SIPLUSNET), todas las versiones;
  - X-200IRT switch family (incluidas las variantes SIPLUSNET), todas las versiones;

    - X-300 switch family (incluidas las variantes X408 y SIPLUS NET), todas las versiones.
- SIDOOR ATD430W, ATE530S COATED y ATE531S, todas las versiones;
- SIMATIC CP 1242-7, todas las versiones anteriores a la versión 3.2;
- SIMATIC CP 1243-1 (incluidas las variantes SIPLUS NET), todas las versiones anteriores a la versión 3.2;
- SIMATIC CP 1243-7 LTE EU, todas las versiones anteriores a la versión 3.2;
- SIMATIC CP 1243-7 LTE US, todas las versiones anteriores a la versión 3.2;
- SIMATIC CP 1243-8 IRC, todas las versiones anteriores a la versión 3.2;
- SIMATIC CP 1542SP-1 IRC (incluidas las variantes SIPLUS NET), todas las versiones anteriores a la versión 2.1;
- SIMATIC CP 1542SP-1, todas las versiones anteriores a la versión 2.1;
- SIMATIC CP 1543-1 (incluidas las variantes SIPLUS NET), todas las versiones anteriores a la versión 2.2;
- SIMATIC CP 1543SP-1 (incluidas las variantes SIPLUS NET), todas las versiones anteriores a la versión 2.1;
- SIMATIC CP 443-1 (incluidas las variantes SIPLUS NET), todas las versiones;
- SIMATIC CP 443-1 Advanced (incluidas las variantes SIPLUS NET), todas las versiones;
- SIMATIC ET 200SP Interfacemodul IM 155-6 MF HF, todas las versiones;
- SIMATIC ET 200SP Open Controller CPU 1515SP PC (incluidas las variantes SIPLUS), todas las versiones anteriores a la versión 2.0;
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incluidas las variantes SIPLUS), todas las versiones anteriores a la versión 2.0;
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incluidas las variantes SIPLUS), todas las versiones de BIOS anteriores a la versión 2.08;
- SIMATIC ET200MP IM155-5 PN HF (incluidas las variantes SIPLUS), versión 4.2 y anteriores;
- SIMATIC ET200SP IM155-6 PN HA (incluidas las variantes SIPLUS), todas las versiones;
- SIMATIC ET200SP IM155-6 PN HF (incluidas las variantes SIPLUS), versión 4.2 y anteriores;
- SIMATIC ET200SP IM155-6 PN/2 HF (incluidas las variantes SIPLUS), versión 4.2 y anteriores;
- SIMATIC ET200SP IM155-6 PN/3 HF (incluidas las variantes SIPLUS), versión 4.2 y anteriores;
- SIMATIC Field PG M4, PG M5 y PG M6, todas las versiones;
- SIMATIC IPC127E, todas las versiones de BIOS anteriores a la versión 27.01.04;
- SIMATIC IPC427C, todas las versiones;
- SIMATIC IPC427D (incluidas las variantes SIPLUS), todas las versiones;
- SIMATIC IPC427E (incluidas las variantes SIPLUS), todas las versiones;
- SIMATIC IPC477C, todas las versiones;
- SIMATIC IPC477D, todas las versiones;
- SIMATIC IPC477E Pro, todas las versiones;
- SIMATIC IPC477E, todas las versiones;
- SIMATIC IPC527G, todas las versiones;
- SIMATIC IPC547E, todas las versiones;
- SIMATIC IPC547G, todas las versiones;
- SIMATIC IPC627C, todas las versiones;
- SIMATIC IPC627D, todas las versiones;
- SIMATIC IPC627E, todas las versiones de BIOS anteriores a la versión 25.02.05;
- SIMATIC IPC647C, todas las versiones;
- SIMATIC IPC647D, todas las versiones;
- SIMATIC IPC647E, todas las versiones de BIOS anteriores a la versión 25.02.05;
- SIMATIC IPC677C, todas las versiones;
- SIMATIC IPC677D, todas las versiones;
- SIMATIC IPC677E, todas las versiones de BIOS anteriores a la versión 25.02.05;
- SIMATIC IPC827C, todas las versiones;
- SIMATIC IPC827D, todas las versiones;
- SIMATIC IPC827E, todas las versiones;
- SIMATIC IPC847C, todas las versiones;
- SIMATIC IPC847D, todas las versiones;
- SIMATIC IPC847E, todas las versiones de BIOS anteriores a la versión 25.02.05;
- SIMATIC ITP1000, todas las versiones;
- SIMATIC MICRO-DRIVE PDC, todas las versiones;
- SIMATIC PN/PN Coupler (incluidas las variantes SIPLUS NET), versión 4.2 y anteriores;
- SIMATIC RF180C, todas las versiones;
- SIMATIC RF182C, todas las versiones;
- SIMATIC RF185C, todas las versiones;
- SIMATIC RF186C y RF186CI, todas las versiones;
- SIMATIC RF188C y RF188CI, todas las versiones;
- SIMATIC S7-1500 CPU family (incluidas las variantes related ET200 CPUs y SIPLUS), todas las versiones anteriores a la versión 2.0;
- SIMATIC S7-1500 Software Controller, todas las versiones anteriores a la versión 2.0;
- SIMATIC S7-300 CPU family (incluidas las variantes related ET200 CPUs y SIPLUS), todas las versiones;
- SIMATIC S7-400 PN/DP V7 y CPU family inferiores (incluidas las variantes SIPLUS), todas las versiones;
- SIMATIC S7-410 CPU family (incluidas las variantes SIPLUS), todas las versiones;
- SIMATIC TDC CP51M1, todas las versiones;
- SIMATIC TDC CPU555, todas las versiones;
- SIMATIC WinAC RTX (F) 2010, todas las versiones;
- SIMOTION P320-4E, todas las versiones;
- SIMOTION P320-4S, todas las versiones;
- SINAMICS S/G Control Unit w. PROFINET, todas las versiones;
- SINEMA Remote Connect Server, todas las versiones >V1.1 y < V2.0.1;
- TIM 3V-IE (incluidas las variantes SIPLUS NET), todas las versiones anteriores a la versión 2.8;
- TIM 3V-IE Advanced (incluidas las variantes SIPLUS NET), todas las versiones anteriores a la versión 2.8;
- TIM 3V-IE DNP3 (incluidas las variantes SIPLUS NET), todas las versiones anteriores a la versión 3.3;
- TIM 4R-IE (incluidas las variantes SIPLUS NET), todas las versiones anteriores a la versión 2.8;
- TIM 4R-IE DNP3 (incluidas las variantes SIPLUS NET), todas las versiones anteriores a la versión 3.3.

Descripción:

Este aviso contiene 10 vulnerabilidades que afectan a múltiples productos de Siemens, de las cuales 2 son de severidad crítica, 6 de severidad alta y 2 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 hay que 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:

- generar una condición de Denegación de Servicio (DoS);

- obtener el control del dispositivo;
- escalada de privilegios;
- revelar información;
- ejecución remota de código.

Se han reservado los siguientes identificadores para estas vulnerabilidades: CVE-2019-19301, CVE-2019-10939, CVE-2018-5390, CVE-2018-5391, CVE-2019-0151, CVE-2019-0152, CVE-2019-0169, CVE-2019-19300, CVE-2020-7574 y CVE-2020-7575.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en HMiSoft VU3 de Eaton

Fecha de publicación: 15/04/2020

Importancia: Alta

Recursos afectados:

HMiSoft VU3, versión 3.00.23 y anteriores.

Descripción:

Natnael Samson, trabajando conjuntamente con ZDI de Trend Micro, ha reportado al CISA dos vulnerabilidades, una de severidad alta y otra media, de desbordamiento de búfer basado en pila y lectura fuera de límites.

Solución:

Eaton dejó de fabricar el producto afectado el 31/12/2018, por lo que ya no proporciona, actualmente, servicio técnico, ni correcciones de seguridad. HMiVU fue reemplazado por la gama de productos XV100 y XV300. Se recomienda que los usuarios de HMiVU se pongan en contacto con Eaton para obtener asistencia técnica y de migración a la solución XV.

Detalle:

- Un archivo de entrada, especialmente diseñado, puede causar un desbordamiento del búfer de la pila (*stack*) cuando el producto afectado lo carga. Se ha reservado el identificador CVE-2020-10639 para esta vulnerabilidad.
- Un archivo de entrada, especialmente diseñado, podría desencadenar una lectura fuera de los límites cuando el producto afectado lo cargue. Se ha reservado el identificador CVE-2020-10637 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en dispositivos de Triangle MicroWorks

Fecha de publicación: 15/04/2020

Importancia: Crítica

Recursos afectados:

- Componentes DNP3 Outstation .NET Protocol, y librerías DNP3 Outstation ANSI C, desde la versión 3.16.00, hasta la versión 3.25.01.
- SCADA Data Gateway:
  - desde la versión 3.02.0697, hasta la versión 4.0.1.22;
  - desde la versión 2.41.0213, hasta la versión 4.0.1.22.

Descripción:

Los investigadores Steven Seely y Chris Anastasio, en colaboración con ZDI de Trend Micro, han reportado a Triangle MicroWorks 4 vulnerabilidades, dos de ellas de severidad crítica, una vulnerabilidad de criticidad alta y otra de criticidad media. Un atacante remoto, no autenticado, podría detener la ejecución de código, ejecutar código arbitrario o generar una condición de denegación de servicio (DoS).

Solución:

- Actualizar DNP3 Outstation .NET Protocol y DNP3 Outstation ANSI C a la versión 3.26.
- Actualizar SCADA Data Gateway a la versión 4.0.123.

Detalle:

Una vulnerabilidad de severidad crítica en DNP3 Outstation podría permitir a un atacante remoto, no autenticado, que enviase un mensaje especialmente diseñado, realizar un desbordamiento de búfer basado pila que podría detener la ejecución de código en el equipo. Se ha reservado el identificador CVE-2020-6996 para esta vulnerabilidad.

Una vulnerabilidad de severidad crítica en SCADA Data Gateway podría permitir a un atacante remoto, no autenticado, la ejecución de código arbitrario debido a una falta de validación de los datos suministrados por el usuario. Se ha reservado el identificador CVE-2020-10611 para esta vulnerabilidad.

Una vulnerabilidad de severidad alta en SCADA Data Gateway podría permitir a un atacante remoto, no autenticado, generar una condición de denegación de servicio (DoS), debido a la falta de validación de la longitud de los datos suministrados por el usuario. Se ha reservado el identificador CVE-2020-10615 para esta vulnerabilidad.

A la vulnerabilidad de severidad media se ha reservado el identificador CVE-2020-10615.

Etiquetas: Actualización, SCADA, Vulnerabilidad

Boletín de seguridad de Schneider Electric de abril de 2020

Fecha de publicación: 15/04/2020

Importancia: Alta

Recursos afectados:

- SoMachine, SoMachine Basic y SoMachine Motion, todas las versiones;
- EcoStruxure Machine Expert y Basic, todas las versiones;
- Modicon M100/M200/M218/M221/M241/M251/M258 Logic Controller, todas las versiones;
- Vijeo Designer Basic, versión 1.1 HotFix 15 y anteriores;
- Vijeo Designer, versión 6.9 SP9 y anteriores;
- TriStation TS1131, versiones desde 4.0.0 hasta 4.9.0, y 4.10.0, ejecutándose en Windows NT, Windows XP y Windows 7;
- Tricon, versiones 10.0, 10.1, 10.2.x y 10.3.x;
- Tricon Communications Module, modelos 4351, 4352, 4351A/B y 4352A/B.

Descripción:

Seok Min Lim y Johnny Pan, de Trustwave, Rongkuan Ma, Shunkai Zhu y Peng Cheng, de 307Lab y de Zhejiang University, Yongjun Liu, de nsfocus y otro investigador independiente han reportado 8 vulnerabilidades a Schneider Electric, con severidades altas y medias, de neutralización inadecuada de elementos en la salida, validación insuficiente de la autenticidad de los datos, transmisión sin cifrar de datos sensibles, ruta de búsqueda no confiable, denegación de servicio y acceso inadecuado al *host*.

Solución:

Seguir las instrucciones de actualización y configuración descritas en la sección *Remediation / Available Remediations* de cada aviso del fabricante.

Detalle:

Un atacante que aproveche estas vulnerabilidades podría realizar las siguientes acciones:

- transferencia de código malicioso al controlador,
- ejecución de código malicioso,
- fuga de información sensible,
- ejecución de código arbitrario,
- enviar información confidencial en claro,
- denegación de servicio (DoS),
- acceso inadecuado a la máquina *host*;
- reseteo de módulos en condiciones de alto tráfico en la red.

Para estas vulnerabilidades, se han reservado los siguientes identificadores: CVE-2020-7489, CVE-2020-7487, CVE-2020-7488, CVE-2020-7490, CVE-2020-7483, CVE-2020-7484, CVE-2020-7485 y CVE-2020-7486.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Envío de mensajes maliciosos en comunicaciones de clientes .NET en OPC UA

Fecha de publicación: 17/04/2020

Importancia: Alta

Recursos afectados:

OPC UA .NET Standard Stack y Sample Code.

Descripción:

Los investigadores, Steven Seeley y Chris Anastasio, trabajando con ZDI de Trend Micro, han descubierto una vulnerabilidad, de severidad alta, que podría causar que un servidor se desconectara al recibir mensajes incorrectos.

Solución:

Aplicar el parche de seguridad o actualizar el paquete NuGet a la versión 1.4.360.33.

Detalle:

El envío de mensajes especialmente diseñados podría desconectar los servidores de OPC UA. Se ha reservado el identificador CVE-2020-8867 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en productos ABB

Fecha de publicación: 22/04/2020

Importancia: Crítica

Recursos afectados:

- OPC Server for AC 800M, todas las versiones;
- MMS Server for AC 800M, todas las versiones;
- Base Software for SoftControl, todas las versiones;
- 800xA for DCI, todas las versiones;
- 800xA for MOD300, todas las versiones;
- 800xA RNRP, todas las versiones;
- ABB System 800xA Base, todas las versiones;
- 800xA Batch Management, todas las versiones;
- 800xA Information Management, todas las versiones;
- ABB Ability™ System 800xA y extensiones de sistemas relacionados 5.1, 6.0 y 6.1;
- Compact HMI 5.1, 6.0;
- Control Builder Safe 1.0, 1.1 y 2.0;
- ABB Ability™ Symphony® Plus - S Operations, desde la 3.0 a la 3.2;
- ABB Ability™ Symphony® Plus - S Engineering, desde la 1.1 a la 2.2;
- Composer Harmony 5.1, 6.0 y 6.1;
- Composer Melody, versiones Melody Composer 5.3, Melody Composer 6.1 / 6.2 y SPE for Melody 1.0 SPx (Composer 6.3);
- Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 y 7.0;
- ABBAbility ™ System 800xA / Advant® OCS Control Builder A, 1.3 y 1.4;
- Advant® OCS AC 100 OPC Server 5.1, 6.0 y 6.1;
- Composer CTK, CTK 6.1, 6.2;
- AdvaBuild, versiones 3.7 SP1 y 3.7 SP2;
- OPC Server for MOD300 (non-800xA), 1.4;
- OPC DataLink 2.1, 2.2;
- ABB Ability™ Knowledge Manager 8.0, 9.0 ,9.1;
- ABB Ability™ Manufacturing Operations Management 1812 y 1909;
- ABB Central Licensing System (CLS) en System 800xA versiones 5.1, 6.0 y 6.1;
- ABB Central Licensing System (CLS) en Compact HMI versiones 5.1 y 6.0;
- ABB Central Licensing System (CLS) en Control Builder Safe versiones 1.0,1.1 y 2.0.

Descripción:

Se han publicado múltiples vulnerabilidades en productos ABB, dos de severidad crítica, seis altas y cinco medias, que podrían permitir a un atacante obtener el control completo del sistema, acceder al servidor de licencias, bloquear el manejo de licencias, modificar las licencias asignadas al sistema de nodos, escalar privilegios, ejecutar código arbitrario, hacer accesible el nodo del sistema o manipular los datos en tiempo de ejecución del sistema.

Solución:

Los productos se actualizarán próximamente. Mientras tanto, deberán tomarse las medidas de mitigación disponibles en la sección de *Referencias*.

Detalle:

- La información confidencial almacenada en ficheros no protegidos podría permitir a un atacante obtener el control completo del sistema. Se ha reservado el identificador CVE-2020-8481 para esta vulnerabilidad de severidad crítica.
- Una vulnerabilidad del tipo inyección de Entidad Externa XML, podría permitir a un atacante leer o llamar a archivos arbitrarios desde el servidor de licencias y/o desde la red o bloquear el manejo de la licencia. Se ha reservado el identificador CVE-2020-8479 para esta vulnerabilidad de severidad crítica.
- Una vulnerabilidad de permisos inadecuados de archivos podría permitir a un atacante bloquear el manejo de licencias, escalar privilegios o ejecutar código arbitrario. Se ha reservado el identificador CVE-2020-8471 para esta vulnerabilidad de severidad alta.
- Una vulnerabilidad de denegación de servicio podría permitir a un atacante bloquear el manejo de la licencia. Se ha reservado el identificador CVE-2020-8475 para esta vulnerabilidad de severidad media.
- Una vulnerabilidad de escalada de privilegios podría permitir a un atacante modificar las licencias asignadas al sistema de nodos. Se ha reservado el identificador CVE-2020-8476 para esta vulnerabilidad de severidad media.
- Existe un riesgo potencial de denegación de servicio o de manipulación en los nodos del Sistema 800xA, que podría permitir a un atacante hacer accesible el nodo del sistema o manipular los datos en tiempo de ejecución del sistema. Se han asignado los identificadores CVE-2020-8478, CVE-2020-8484, CVE-2020-8485, CVE-2020-8486, CVE-2020-8487, CVE-2020-8488 y CVE-2020-8489 para estas vulnerabilidades de severidades medias y altas.

Etiquetas: Vulnerabilidad

Acceso no controlado a rutas en UPS Adapter CS141 de ABB

Fecha de publicación: 24/04/2020

Importancia: Media

Recursos afectados:

- La siguiente lista de dispositivos UPS Adapter CS141, con versiones de *firmware* desde la 1.66 hasta la 1.88:
  - CS141 Advanced - Box;
  - CS141 Advanced - Slot;
  - CS141 ModBus - Box;
  - CS141 ModBus - Slot;
  - CS141 Basic - Box;
  - CS141 Basic - Slot.

Descripción:

El investigador de ciberseguridad, Eduardo Cataño Conde, ha reportado a ABB una vulnerabilidad de criticidad media, que podría permitir a un atacante remoto, acceso no controlado a rutas y obtener información del dispositivo afectado.

Solución:

Actualizar los productos afectados a la versión de *firmware* 1.90.

Detalle:

Un atacante con credenciales de administrador, o ingeniero, podría manipular las variables que referencian a los archivos para acceder a directorios y archivos fuera del directorio «web». Se ha reservado el identificador CVE-2020-11420 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Divulgación de información en NPort 5100A Series de Moxa

Fecha de publicación: 29/04/2020

Importancia: Media

Recursos afectados:

NPort 5100A Series, versión del *firmware* 1.5 o anterior.

Descripción:

Se ha publicado una vulnerabilidad en los productos NPort 5100A Series de Moxa que podría permitir a un atacante, no autenticado, realizar una divulgación de información.

Solución:

- Actualizar a la versión del *firmware* 1.51 o siguientes.
- Desactivar la opción "Moxa Service" de la consola de ajustes. En caso de necesitar esta opción, añadir los dispositivos que necesiten acceso a una lista blanca y activar la opción 'Apply additional restrictions' en la configuración de listas de "Accessible IP List".

Detalle:

La vulnerabilidad podría permitir a un atacante no autenticado obtener las configuraciones del puerto serie del dispositivo. Se ha reservado el identificador CVE-2020-12117 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad