Boletín de febrero de 2020

Avisos de Sistemas de Control Industrial

Credenciales insuficientemente protegidas en C-more Touch Panels de AutomationDirect

Fecha de publicación: 05/02/2020

Importancia: Crítica

Recursos afectados:

C-More Touch Panels EA9 series, versiones de *firmware* anteriores a 6.53.

Descripción:

El investigador Joel Langill, de Amentum Mission Engineering & Resilience, ha reportado una vulnerabilidad, de tipo credenciales insuficientemente protegidas, que podría permitir a un atacante obtener información de la cuenta, como nombres de usuario y contraseñas, ocultar o manipular datos del proceso y bloquear el acceso al dispositivo.

Solución:

El fabricante recomienda la actualización a la versión 6.53.

Detalle:

La vulnerabilidad identificada podría permitir a un atacante remoto desenmascarar las credenciales y otra información sensible en archivos de proyectos desprotegidos, otorgando acceso al sistema y la capacidad de manipular su configuración. Se ha reservado el CVE-2020-6969 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

Desbordamiento de búfer en bombillas inteligentes de Philips

Fecha de publicación: 05/02/2020

Importancia: Alta

Recursos afectados:

Bombillas inteligentes Philips HUE.

Descripción:

Los investigadores de Check Point han reportado una vulnerabilidad, de tipo desbordamiento de búfer basado en memoria dinámica (Heap), que podría permitir a un atacante instalar código malicioso en el puente de control del firmware.

Solución:

Se ha publicado la versión 1935144040 del firmware de los productos afectados que soluciona esta vulnerabilidad. La instalación de la actualización es automática, no obstante, se aconseja comprobar que se ha actualizado el dispositivo. En caso contrario deberá hacerse de forma manual.

Detalle:

La vulnerabilidad identificada podría permitir a un atacante tomar el control sobre la red IoT de las bombillas, mediante el envío de grandes cantidades de datos al puente de control. Esto le permitiría lanzar ataques de malware a redes informáticas en empresas o

incluso en ciudades inteligentes. Se ha reservado el CVE-2020-6007 para esta vulnerabilidad.

Etiquetas: IoT, Vulnerabilidad

Múltiples vulnerabilidades en LANTIME de Meinberg

Fecha de publicación: 10/02/2020

Importancia: Crítica

Recursos afectados:

- Todas las versiones del *firmware* de LANTIME anteriores a la V6.24.024 (V7.00.002 respectivamente), con excepción de CVE-2019-1551 y NO-CVE13 que también afectan a todas las versiones anteriores a la V7.00.006;
- Todos los dispositivos de la serie M de LANTIME (M100, M200, M300, M400, M600, M900);
- Todos los dispositivos de la serie IMS de LANTIME (M500, M1000, M1000S, M3000, M3000S, M4000);
- Familia de productos SyncFire (SF1000 / SF1100).

Descripción:

Los investigadores Michal Bazyli y Jakub Palaczynski, de Checkpoint, han reportado varias vulnerabilidades de lectura/escritura de archivos arbitrarios, escalada de privilegios, divulgación de información, ejecución remota de código, XSS, debilidad de la caché del navegador, inyección en línea de comandos, desbordamiento de búfer, falta de cifrado de información sensible y contraseña SSH por defecto.

Solución:

Actualizar el *firmware* a las versiones V7.00.006 y V6.24.024 desde el centro de descargas para corregir las vulnerabilidades listadas, a excepción de la vulnerabilidad con identificador CVE-2020-7240.

Detalle:

A continuación, se detallan las vulnerabilidades de severidad crítica:

- Los usuarios no autentificados pueden modificar el código de Java Script a través del diálogo de inicio de sesión que fue entregado por el servidor web a través de la función *System* ? *System Information* ? *Show System Messages* mediante un ataque de XSS almacenado y no autenticado.
- El acceso *root* a las tarjetas de la TSU a través de la red fue posible debido a que se mantenía una clave por defecto de SSH.

Para el resto de las vulnerabilidades, se han reservado los identificadores: CVE-2018-10834, CVE-2018-10835 y CVE-2018-10836. Los identificadores asignados son: CVE-2020-7240, CVE-2011-2900, CVE-2019-1563, CVE-2019-1547, CVE-2019-1552 y CVE-2019-1551.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

Vulnerabilidad de XSS en múltiples productos de eWON

Fecha de publicación: 11/02/2020

Importancia: Alta

Recursos afectados:

- Flexy, versiones anteriores a la 14.1s0;
- Cosy, versiones anteriores a la 14.1s0.

Descripción:

Ander Martínez, de Titanium Industrial Security, ha reportado una vulnerabilidad en los dispositivos de eWON que podría permitir a un atacante remoto realizar un ataque CSRF, pudiendo comprometer la máquina del administrador.

Solución:

Actualizar a la versión 14.1s0.

Detalle:

Un atacante podría provocar un cambio de contraseña realizando un ataque CSRF o comprometer la máquina del administrador utilizando alguna vulnerabilidad del navegador. La víctima de XSS debe introducir las credenciales antes de ejecutar el código.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en dispositivos Siemens

Fecha de publicación: 11/02/2020

Importancia: Crítica

Recursos afectados:

- OpenPCS 7, SIMATIC BATCH, SIMATIC PCS 7 y SIMATIC Route Control:
  - V8.1, todas las versiones;
  - V8.2, todas las versiones;
  - V9.0, todas las versiones.
- SIMATIC NET PC Software;
- SIMATIC WinCC (TIA Portal):
  - V13, versiones anteriores a las V13 SP2;
  - V14.0.1, todas las versiones;
  - V15.1, todas las versiones;
  - V16, todas las versiones.
- SIMATIC WinCC:
  - V7.3, todas las versiones;
  - V7.4, todas las versiones;
  - V7.5, versiones anteriores a la V7.5.1 Udp1.
- Familia SIMATIC S7-1200 CPU incluyendo variante SIPLUS, versiones anteriores a la V4.1;
- Familia SIMATIC S7-300 PN/DP CPU, incluyendo variante SIPLUS y relacionados con ET200 CPUs, todas las versiones;
- Familia SIMATIC S7-400 PN/DP V6, incluyendo variante SIPLUS, todas las versiones;
- Familia SIMATIC S7-400 PN/DP V7 CPU y anteriores, incluyendo variante SIPLUS, todas las versiones;
- SCALANCE:
  - S602, todas las versiones;
  - S612, todas las versiones;
  - S623 todas las versiones;
  - S627-2M todas las versiones.
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2, incluyendo variante SIPLUS, todas las versiones;
- Familia SIMATIC S7-1500 CPU, incluyendo variante SIPLUS y relacionados con ET200 CPUs, todas las versiones anteriores a la V2.5, incluida, y las versiones entre la V2.5 y la V2.8;
- SIMATIC S7-1500 Software Controller. Todas las versiones anteriores a la V2.5, incluida, y las versiones entre la V2.5 y la V20.8;
- SIMATIC CP 1623, todas las versiones anteriores a V14.00.15.00_51.25.00.01;
- SIMATIC CP 1626, todas las versiones;
- SIMATIC CP 1628, todas las versiones;
- TIM 1531 IRC (incl. todas las variantes SIPLUS NET), todas las versiones anteriores a V2.0;
- Kit de desarrollo/evaluación para PROFINET IO:
  - DK Standard Ethernet Controller, todas las versiones.;
  - EK-ERTEC 200, versiones anteriores a la V4.5;
  - EK-ERTEC 200P, versiones anteriores a la V4.6.
- PROFINET Driver for Controller, versiones anteriores a la V2.1;
- IE/PB LINK PN IO (incl. todas las variantes SIPLUS NET);
- RUGGEDCOM RM1224, versiones anteriores a la V4.3;
- SIPORT MP, todas las versiones anteriores a 3.1.4;
- OZW672, todas las versiones anteriores a v10.00;
- OZW772, todas las versiones anteriores a v10.00;
- SCALANCE:
  - M-800 / S615, versiones anteriores a la V4.3;
  - W700 IEEE 802.11n, versiones anteriores a la V6.0.1, incluida;
  - Familia de switches X-200 incluyendo variante SIPLUS NET, todas las versiones;
  - Familia de switches X-200IRT, incluyendo variante SIPLUS NET, todas las versiones;
  - Familia de switches X-300 incluyendo variante SIPLUS NET y el X408, todas las versiones;
  - XB-200, XC-200, XP-200, XF-200BA y XR-300WG, versiones anteriores a la V3.0;
  - Familia de switches XM-400, versiones anteriores a la V6.0;
  - Familia de switches XR-500, versiones anteriores a la V6.0.
- SIMATIC:
  - CP 1616 y CP 1604, versiones anteriores a la V2.8;
  - CP 343-1, incluyendo variante SIPLUS NET, todas las versiones;
  - CP 343-1 Advanced, incluyendo variante SIPLUS NET, todas las versiones;
  - CP 343-1 ERPC, todas las versiones;
  - CP 343-1 LEAN, todas las versiones;
  - CP 443-1, incluyendo variante SIPLUS NET, todas las versiones;
  - CP 443-1 Advanced, incluyendo variante SIPLUS NET, todas las versiones;
  - CP 443-1 OPC UA, todas las versiones;
  - ET200AL;
  - ET200ecoPN (excepto 6ES7148-6JD00- 0AB0 y 6ES7146-6FF00-0AB0), todas las versiones;
  - ET200S incluyendo variante SIPLUS, todas las versiones;
  - ET200S incluyendo variante SIPLUS, todas las versiones;
  - ET200M incluyendo variante SIPLUS, todas las versiones;
  - SIMATIC CP 1543-1, versiones anteriores a la V2.0 y entre la V2.0 y V2.2;
  - IPC Support, paquete para VxWork, todas las versiones;
  - Familia MV400, todas las versiones;
  - RF182C, todas las versiones;
  - Familia RF600, versiones anteriores a la V3.
- SINAMICS DCP, versiones anteriores a la V1.3;
- SIPROTEC 4 y los relés SIPROTEC Compact, todas las versiones.

Descripción:

Este aviso contiene 15 vulnerabilidades que afectan a productos de Siemens de las cuales 1 es de severidad crítica, 8 altas y 6 medias.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas, pueden descargarse desde el panel de descarga de Siemens.

Para los productos sin actualizaciones, aplicar las medidas de mitigación descritas en la sección de referencias.

Detalle:

Un atacante que aprovechara alguna de las vulnerabilidades críticas descritas en este aviso, podría llegar a realizar alguna de las siguientes acciones:

- Denegación del servicio,
- Ejecución remota de código,
- Divulgación de información.

Se han asignado los siguientes identificadores para estas vulnerabilidades: CVE-2019-19282, CVE-2019-13925, CVE-2019-3926, CVE-2019-19281, CVE-2019-13946, CVE-2019-12815, CVE-2019-18217, CVE-2019-19279, CVE-2015-5621, CVE-2019-13940, CVE-2019-6585, CVE-2019-13924, CVE-2018-18065, CVE-2019-19277 y CVE-2019-13941.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en ConnectPort LTS 32 MEI de Digi International

Fecha de publicación: 12/02/2020

Importancia: Baja

Recursos afectados:

ConnectPort LTS 32 MEI, versión del firmware 1.4.3 (82002228_K 08/09/2018) y versión de bios 1.2.

Descripción:

Los investigadores, Murat Aydemir y Fatih Kayran, han reportado varias vulnerabilidades en el producto ConnectPort LTS 32 MEI de Digi International que podrían permitir a un atacante limitar la disponibilidad del sistema.

Solución:

Actualizar a la versión 1.4.5.

Detalle:

- La subida sin restricciones de ficheros podría permitir a un atacante introducir código malicioso dentro de la aplicación. Se ha asignado el identificador CVE-2020-6975 para esta vulnerabilidad.
- La neutralización incorrecta de la entrada durante la generación de la página web podría permitir a un atacante causar una condición de denegación de servicio mediante ataques del tipo cross-site scripting. Se ha asignado el identificador CVE-2020-6973 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Ruta de búsqueda no controlada en ProSoft Configurator de Schneider Electric

Fecha de publicación: 12/02/2020

Importancia: Alta

Recursos afectados:

ProSoft Configurator v1.002 y anteriores, para el módulo PMEPXM0100 (H).

Descripción:

El investigador Yongjun Liu (nsfocus) ha descubierto una vulnerabilidad de tipo ruta de búsqueda no controlada que afecta a ProSoft Configurator, que podría permitir a un atacante local ejecutar código arbitrario.

Solución:

Actualizar ProSoft Configurator a la versión v1.003 o posterior.

Detalle:

Una vulnerabilidad de elemento de ruta (*path*) de búsqueda no controlada podría permitir a un atacante local la ejecución de código arbitrario al abrir un proyecto que podría ejecutar una DLL maliciosa. Se ha reservado el identificador CVE-2020-7474 para dicha vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de ABB

Fecha de publicación: 13/02/2020

Importancia: Alta

Recursos afectados:

- Asset Suite, versiones 9.6 y anteriores.
- eSOMS, versiones 6.02 y anteriores.

Descripción:

ABB ha reportado varias vulnerabilidades del tipo: referencia directa a objeto, cabeceras HTTP no activadas correctamente, flags seguros no activados, filtración de información, falta de control de la complejidad de la contraseña, uso de software vulnerable, inyección SQL, falta de validación de entradas y salidas, almacenamiento de contraseñas en claro y uso de algoritmos de encriptación débiles. Estas vulnerabilidades podrían permitir a un atacante acceder a información sensible.

Solución:

Actualizar a las siguientes versiones:

- eSOMS: 6.0.3 y 6.1,
- Asset Suite: 9.4.2.6, 9.5.3.2 y 9.6.1.

Detalle:

Las vulnerabilidades de severidad alta son:

- Un fallo en los controles utilizados para limitar el acceso a los recursos podría permitir a un atacante, que conozca o descubra la URL de un recurso al que no tiene permiso, acceder a dicho recurso buscándolo directamente mediante la URL. Se ha asignado el identificador CVE-2019-18998 para esta vulnerabilidad.
- En eSOMS está instalada una versión de Redis vulnerable.
- La falta de validación de la entrada para los queries SQL, en el eSOMS, podría permitir a un atacante realizar ataques de inyección SQL contra la base de datos interna. Se ha asignado el identificador CVE-2019-19094 para esta vulnerabilidad.

Para el resto de las vulnerabilidades se han asignado los identificadores CVE-2019-19000, CVE-2019-19001, CVE-2019-19002, CVE-2019-19003, CVE-2019-19089, CVE-2019-19090, CVE-2019-19091, CVE-2019-19092, CVE-2019-19093, CVE-2019-19095, CVE-2019-19096 y CVE-2019-19097.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en equipos OnCell de Moxa

Fecha de publicación: 13/02/2020

Importancia: Crítica

Recursos afectados:

- Moxa OnCell G3470A-LTE Series, versiones de *firmware* 1.6 o anteriores.
- Moxa OnCell G3100-HSPA Series, versiones de *firmware*:
  - 1.4 o anteriores para las vulnerabilidades con identificadores CVE-2018-11420, CVE-2018-11423 y CVE-2018-11424;
  - 1.7 o anteriores para las vulnerabilidades con identificadores CVE-2018-11426, CVE-2018-11427, CVE-2018-11421 y CVE-2018-11422.

Descripción:

Alexander Zaytsev, de Kaspersky Lab, ha reportado múltiples de tipo restricción impropia de operaciones, consumo de recursos no controlado, desreferencia del puntero NULL, autenticación inapropiada, CSRF, divulgación de información y control de acceso inadecuado, que afectan a los productos OnCell G3470A-LTE Series y OnCell G3100-HSPA Series de Moxa.

Solución:

- Para OnCell G3470A-LTE Series, descargar la última versión de *firmware* del producto.
- Para OnCell G3100-HSPA Series:
  - descargar la última versión de *firmware* del producto para solucionar las vulnerabilidades con identificadores CVE-2018-11420, CVE-2018-11423, CVE-2018-11424, CVE-2018-11426 y CVE-2018-11427;
  - añadir mecanismos de seguridad como soluciones VPN punto a punto, únicamente cuando están activadas las funcionalidades *OnCell Search Utility* y *OnCell Central Manager* en el producto afectado, para solucionar las vulnerabilidades con identificadores CVE-2018-11421 y CVE-2018-11422.

Detalle:

Un atacante que aprovechara alguna de las vulnerabilidades críticas descritas en este aviso podría llegar a realizar alguna de las siguientes acciones:

- denegación de servicio,
- ejecución remota de código,
- ataques de fuerza bruta contra parámetros de autenticación,
- suplantar acciones administrativas a través de la interfaz web,
- obtención de información sensible,
- modificar configuraciones y subir *firmware*.

Se han asignado los siguientes identificadores: CVE-2018-11420, CVE-2018-11421, CVE-2018-11422, CVE-2018-11423, CVE-2018-11424, CVE-2018-11425, CVE-2018-11426 y CVE-2018-11427.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Acceso no autenticado al servidor web en productos de Phoenix Contact

Fecha de publicación: 14/02/2020

Importancia: Crítica

Recursos afectados:

- Phoenix Contact Emalytics Controllers ILC 2050 BI, hasta la versión de *firmware* 1.21;
- Phoenix Contact Emalytics Controllers ILC 2050 BI-L, hasta la versión de *firmware* 1.21.

Descripción:

Anil Parmar ha descubierto una vulnerabilidad crítica, de configuración remota usando acceso no autenticado a un servidor web, que afecta a varios productos de Phoenix Contact.

Solución:

Actualizar los productos afectados a la versión de *firmware* 1.2.3 o superior.

Detalle:

Un enlace a la web de los dispositivos afectados otorga un acceso no autorizado, con permisos de lectura y escritura, a la configuración de dichos dispositivos, lo que permitiría a un atacante modificar la configuración de los dispositivos e iniciar y detener servicios. Se ha reservado el identificador CVE-2020-8768 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Gestión incorrecta de privilegios en INNCOM INNControl 3 de Honeywell

Fecha de publicación: 19/02/2020

Importancia: Media

Recursos afectados:

INNControl 3, versiones 3.21 y anteriores.

Descripción:

El equipo de Honeywell ha reportado una vulnerabilidad, de tipo gestión incorrecta de privilegios, que afecta a su producto INNCOM INNControl 3.

Solución:

Los usuarios deben ponerse en contacto con un representante de ventas de INNCOM o con un integrador de sistemas autorizado para obtener información sobre la actualización de su sistema a la última versión. Honeywell también ofrece soporte en línea de INNCOM.

Detalle:

La vulnerabilidad detectada, de gestión incorrecta de privilegios, podría permitir a un atacante elevar los privilegios de usuario dentro de la aplicación INNControl mediante la modificación de archivos de configuración local. Se ha reservado el identificador CVE-2020-6968 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

---

Fallo del mecanismo de protección en múltiples productos de GE

Fecha de publicación: 19/02/2020

Importancia: Media

Recursos afectados:

- Vivid, todas las versiones;
- LOGIQ, todas las versiones salvo LOGIQ 100 Pro;
- Voluson, todas las versiones;
- Versana Essential, todas las versiones;
- Invenia ABUS Scan station, todas las versiones;
- Venue todas las versiones, no se incluyen Venue 40 R1-3 y Venue 50 R4-5.

Descripción:

Los investigadores Marc Ruef y Rocco Gagliardi han reportado una vulnerabilidad de tipo fallo del mecanismo de protección que podría permitir a un atacante obtener acceso al sistema operativo del dispositivo afectado.

Solución:

GE Healthcare recomienda a las organizaciones restringir el acceso físico a los dispositivos para personas no autorizadas, además de activar el bloqueo del dispositivo por contraseña en la GUI, si es posible.

Detalle:

Una vulnerabilidad de escape de entorno de escritorio restringido, en la funcionalidad del modo Kiosk, podría permitir a un atacante escapar del entorno restringido y acceder al sistema operativo subyacente, mediante entradas especialmente diseñadas. Se ha asignado el identificador CVE-2020-6977.

Etiquetas: Vulnerabilidad

Desbordamiento de búfer basado en memoria dinámica en OpenEnterprise de Emerson

Fecha de publicación: 19/02/2020

Importancia: Alta

Recursos afectados:

- OpenEnterprise Server 2.83 está afectado si los protocolos Modbus o ROC Interfaces han sido instalados y están en uso;
- OpenEnterprise, desde 3.1 hasta 3.3.3, todas las versiones.

Descripción:

Roman Lozko, de Kaspersky ICS CERT, ha informado de una vulnerabilidad de desbordamiento de búfer basado en memoria dinámica (*heap*), que afecta al producto OpenEnterprise de Emerson.

Solución:

Actualizar OpenEnterprise a la versión 3.3 SP4 (3.3.4), disponible desde la web de soporte de Emerson.

Detalle:

Un *script*, especialmente diseñado, puede servir para ejecutar código en el servidor de OpenEnterprise, generando un desbordamiento de búfer basado en memoria dinámica (*heap*). Se ha reservado el identificador CVE-2020-6970 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

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

---

Múltiples vulnerabilidades en Notifier Web Server (NWS-3) de Honeywell

Fecha de publicación: 21/02/2020

Importancia: Crítica

Recursos afectados:

Honeywell Notifier Web Server (NWS-3), versiones 3.50 y anteriores.

Descripción:

Gjoko Krstikj ha reportado dos vulnerabilidades, ambas de severidad crítica, de tipos omisión de autenticación por captura y repetición del tráfico de red, y acceso a rutas no controlado.

Solución:

Actualizar el producto afectado a la versión de *firmware* 4.51.

Detalle:

- La autentificación en Honeywell Fire Web Server puede ser omitida por un ataque de captura y repetición del tráfico de red desde un navegador web. Se ha reservado el identificador CVE-2020-6972 para esta vulnerabilidad.
- El producto afectado es vulnerable a un ataque de acceso a rutas no controlado, lo que permitiría a un atacante omitir el acceso a directorios restringidos. Se ha reservado el identificador CVE-2020-6974 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en FactoryTalk Diagnostics de Rockwell Automation

Fecha de publicación: 21/02/2020

Importancia: Crítica

Recursos afectados:

- FactoryTalk Diagnostics, todas las versiones.

Descripción:

Se ha reportado una vulnerabilidad de tipo deserialización de datos no confiables que podría permitir a un atacante la ejecución de código arbitrario con los privilegios de SYSTEM.

Solución:

Rockwell Automation está trabajando en una actualización. Hasta entonces, se recomienda:

- Deshabilitar el servicio de Remote Diagnostics si no se utiliza;
- Si el servicio está en uso, utilizar un firewall para deshabilitar el puerto afectado,

Detalle:

Factory Talk Diagnostics expone un Remoting endpoint .NET, a través de RNADiagnosticsSrv.exe en TCP/8082, que puede deserializar de forma insegura datos no confiables. Se ha asignado el identificador CVE-2020-6967.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en AWK-3131A Series de MOXA

Fecha de publicación: 24/02/2020

Importancia: Alta

Recursos afectados:

AWK-3131A Series, versiones del *firmware* 1.13 y anteriores.

Descripción:

Se han reportado una serie de vulnerabilidades, en productos de Moxa, del tipo control de acceso inapropiado, uso de contraseñas embebidas, neutralización inapropiada de elementos especiales utilizados en comandos del sistema operativo, copia del búfer sin comprobación del tamaño de entrada, lectura fuera de límites, desbordamiento de búfer basado en pila (*stack*) y evasión de autenticación mediante canal o ruta alternativa.

Solución:

Contactar con el soporte técnico de Moxa para obtener la actualización.

Detalle:

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

- Envío de comandos. Se han reservado los identificadores CVE-2019-5136 y CVE-2019-5162 para estas vulnerabilidades.
- Descifrar el tráfico capturado. Se ha reservado el identificador CVE-2019-5137 para esta vulnerabilidad.
- Inyección de comandos para obtener el control del dispositivo. Se han reservado los identificadores CVE-2019-5138, CVE-2019-5140, CVE-2019-5141 y CVE-2019-5142 para estas vulnerabilidades.
- Uso de contraseñas embebidas. Se ha reservado el identificador CVE-2019-5139 para esta vulnerabilidad.
- Ejecución remota de código. Se han reservado los identificadores CVE-2019-5143 y CVE-2019-5153 para estas vulnerabilidades.
- Denegación del servicio. Se ha reservado el identificador CVE-2019-5148 para esta vulnerabilidad.
- Evasión de autenticación. Se ha reservado el identificador CVE-2019-5165 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Honeywell WIN-PAK

Fecha de publicación: 26/02/2020

Importancia: Alta

Recursos afectados:

WIN-PAK, versión 4.7.2 y anteriores.

Descripción:

Se han detectado 3 vulnerabilidades, 2 de severidad alta y una media, de tipos CSRF, neutralización inadecuada de los encabezados HTTP para la sintaxis de los *scripts* y uso de librerías obsoletas.

Solución:

Actualizar WIN-PAK a la versión 4.7.2 B1072.3.4 y, posteriormente, aplicar el parche.

Detalle:

- El producto afectado es vulnerable a CSRF (C*ross-Site Request Forgery*), lo que puede permitir a un atacante remoto ejecutar código arbitrario. Se ha reservado el identificador CVE-2020-7005 para esta vulnerabilidad.
- Se ha identificado una vulnerabilidad de neutralización incorrecta de las cabeceras HTTP, que puede permitir la ejecución remota de código. Se ha reservado el identificador CVE-2020-6982 para esta vulnerabilidad.
- El producto afectado es vulnerable debido al uso de librerías jQuery obsoletas. Se ha reservado el identificador CVE-2020-6978 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en productos de Moxa

Fecha de publicación: 26/02/2020

Importancia: Crítica

Recursos afectados:

- Las siguientes pasarelas de protocolos:
  - Series MB3170, con versión de firmware 4.0 o anterior;
  - Series MB3270, con versión de firmware 4.0 o anterior;
  - Series MB3180, con versión de firmware 2.0 o anterior;
  - Series MB3280, con versión de firmware 3.0 o anterior;
  - Series MB3480, con versión de firmware 3.0 o anterior;
  - Series MB3660, con versión de firmware 2.2 o anterior;
- Series ioLogik 2500, con versión de firmware 3.0 o anterior;
- IOxpress servicio de configuración, versión 2.3.0 o anterior;
- Los switches ethernet:
  - Series PT-7528,con versión de firmware 4.0 o anterior;
  - Series PT-7828, con versión de firmware 3.9 o anterior;
  - Series DS-G516E, con versión de firmware5.2 o anterior;
  - Series EDS-510E, con versión de firmware 5.2 o anterior;

Descripción:

Diversos investigadores han reportado a Moxa veinticinco vulnerabilidades, una de severidad baja, seis de severidad media, ocho altas y diez críticas. Un atacante remoto podría ejecutar código arbitrario, saltarse restricciones de acceso y realizar modificaciones de configuraciones afectando a la confidencialidad, integridad y disponibilidad.

Solución:

- Para las Series EDS-G516E, se recomienda actualizar a la última versión disponible.
- MOXA ha desarrollado una nueva versión de firmware para los modelos: MB3170, MB3270, MB3180, MB3280, MB3480 y MB3660. Para obtenerla, póngase en contacto directamente con el fabricante para su actualización.
- Para el resto de los dispositivos consulte con el servicio de soporte técnico de Moxa.

Detalle:

- Un atacante podría ejecutar código arbitrario, dejando fuera de servicio al dispositivo. Se han reservado los identificadores CVE-2020-7007, CVE-2020-6989 y CVE-2019-9099 para estas vulnerabilidades.
- Los productos afectados utilizan claves criptográficas embebidas, que podría permitir que se revele información confidencial. Se han reservado los identificadores CVE-2020-6979 y CVE-2020-6983 para estas vulnerabilidades.
- Un atacante podría conseguir acceso al sistema sin la autorización adecuada. Se han reservado los identificadores CVE-2020-6981 y CVE-2020-6985 para estas vulnerabilidades.
- Un atacante podría acceder al sistema utilizando fuerza bruta. Se han reservado los identificadores CVE-2020-6991, CVE-2020-6995 y CVE-2019-9096 para estas vulnerabilidades.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2020-7001, CVE-2020-6989, CVE-2020-6997, CVE-2020-6987, CVE-2020-6993, CVE-2019-18238, CVE-2020-7003, CVE-2019-18242, CVE-2019-9098, CVE-2019-9102, CVE-2019-9095, CVE-2019-9103, CVE-2019-9101, CVE-2019-9104 y CVE-2019-9097.

Etiquetas: Actualización, Vulnerabilidad

Desbordamiento de búfer en WebAccess/SCADA

de Advantech

Fecha de publicación: 27/02/2020

Importancia: Crítica

Recursos afectados:

Advantech WebAccess/SCADA, versión 8.4.3.

Descripción:

Se ha identificado una vulnerabilidad con severidad crítica de tipo desbordamiento de búfer que afecta al software WebAccess/SCADA de Advantech. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código arbitrario.

Solución:

Advantech ha publicado la versión 9.0 del software que soluciona esta vulnerabilidad.

Detalle:

En la librería BwPAlarm.dll no se hace una correcta validación de los datos de usuario cuando se procesan mensajes de tipo IOCTL 70022 RPC. Esto podría permitir a un atacante remoto controlar tamaño del búfer de la pila y los datos copiados en este.

Etiquetas: Actualización, SCADA, Vulnerabilidad