Boletín de enero de 2021

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en productos Pepperl Fuchs

Fecha de publicación: 05/01/2021

Importancia: Alta

Recursos afectados:

Versiones de firmware 1.5.48 y anteriores, de P F Comtrol:

- IO-Link Master 4-EIP,
- IO-Link Master 8-EIP,
- IO-Link Master 8-EIP-L,
- IO-Link Master DR-8-EIP,
- IO-Link Master DR-8-EIP-P,
- IO-Link Master DR-8-EIP-T,
- IO-Link Master 4-PNIO,
- IO-Link Master 8-PNIO,
- IO-Link Master 8-PNIO-L,
- IO-Link Master DR-8-PNIO,
- IO-Link Master DR-8-PNIO-P,
- IO-Link Master DR-8-PNIO-T.

Descripción:

T.Weber, de SEC Consult Vulnerability Lab, ha reportado esta vulnerabilidad, coordinada por el , que podría permitir a un atacante acceder al dispositivo y a su información, o ejecutar programas.

Solución:

Actualizar los productos afectados con los siguientes paquetes de firmware:

- U-Boot bootloader, versión 1.36 o posterior;
- System image, versión 1.52 o posterior;
- Application base, 1.6.11 o posterior.

Además, para productos que estén conectados a una red pública, el fabricante recomienda:

- Poner en práctica medidas de protección externa.
- El tráfico de las redes no confiables al dispositivo debe ser bloqueado por cortafuegos, especialmente el tráfico dirigido a la página de administración.
- Las cuentas de usuario del dispositivo deben habilitarse con contraseñas seguras.
- Si personas o aplicaciones no confiables tienen acceso a la red a la que está conectado el dispositivo, se recomienda configurar las contraseñas de las tres cuentas de usuario.

Detalle:

Las vulnerabilidades identificadas son del tipo:

- Cross-Site Request Forgery (CSRF). Se ha asignado el identificador CVE-2020-12511 para esta vulnerabilidad de severidad alta.
- Cross-Site Scripting (XSS). Se ha asignado el identificador CVE-2020-12512 para esta vulnerabilidad de severidad alta.
- Neutralización inapropiada de elementos especiales utilizados en un comando del Sistema Operativo (OS Command Injection). Se ha asignado el identificador CVE-2020-12513 para esta vulnerabilidad de severidad alta.
- Desreferencia del puntero NULL. Se ha asignado el identificador CVE-2020-12514 para esta vulnerabilidad de severidad media.

- Lectura fuera de límites. Se ha asignado el identificador CVE-2018-20679 para esta vulnerabilidad de severidad alta.
- Errores en la administración de claves. Se ha asignado el identificador CVE-2018-0732 para esta vulnerabilidad de severidad media.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Schneider Electric

Fecha de publicación: 07/01/2021

Importancia: Alta

Recursos afectados:

Los siguientes productos Modicon:

- M340 CPUs:
  - BMX P34x, todas las versiones.
- Módulos M340 Communication Ethernet:
  - BMX NOE 0100 (H), todas las versiones;
  - BMX NOE 0110 (H), todas las versiones;
  - BMX NOC 0401, todas las versiones;
  - BMX NOR 0200H, todas las versiones.
- Premium processors, con Ethernet COPRO integrado:
  - TSXP574634, TSXP575634, TSXP576634, todas las versiones.
- Módulos de comunicación Premium:
  - TSXETY4103, todas las versiones;
  - TSXETY5103, todas las versiones.
- Procesadores Quantum con Ethernet COPRO integrado:
  - 140CPU65xxxxx, todas las versiones.
- Módulos de comunicación Quantum:
  - 140NOE771x1, todas las versiones;
  - 140NOC78x00, todas las versiones;
  - 140NOC77101, todas las versiones.

Descripción:

Kai Wang, de Fortinet's FortiGuard Labs, ha reportado estas vulnerabilidades a Schneider Electric que podrían permitir a un atacante corromper datos o provocar la caída del servidor web.

Solución:

Está prevista una actualización de los controladores Modicon PAC. Hasta que esté disponible, el fabricante recomienda:

- Deshabilitar el FTP a través de UnityPro / Ecostruxure Control Expert. Esta opción está desactivada por defecto cuando se crea una nueva aplicación.
- Configurar la lista de control de acceso a través de la herramienta de programación Ecostruxure Control Expert.
- Configurar la segmentación de la red e implementar un cortafuegos para bloquear todo acceso no autorizado al puerto 21/TCP.

Los controladores Modicon Premium y Modicon Quantum de Schneider Electric han llegado al final de su vida útil y ya no están disponibles comercialmente. Han sido reemplazados por el controlador ePAC Modicon M580.

Detalle:

- Una vulnerabilidad de lectura fuera de límites, podría causar un fallo de segmentación o un desbordamiento del búfer cuando se sube un archivo especialmente diseñado en el controlador, a través de FTP. Se ha asignado el identificador CVE-2020-7562 para esta vulnerabilidad.
- Una vulnerabilidad de escritura fuera de límites, podría causar la corrupción de los datos, una caída o la ejecución de código cuando se sube un archivo especialmente diseñado en el controlador, a través de FTP. Se ha asignado el identificador CVE-2020-7563 para esta vulnerabilidad.
- Una vulnerabilidad de desbordamiento del búfer, podría causar el acceso de escritura y la ejecución de comandos cuando se sube un archivo especialmente diseñado en el controlador, a través de FTP. Se ha asignado el identificador CVE-2020-7564 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Schneider Electric, Windows

---

Múltiples vulnerabilidades en productos de General Electric

Fecha de publicación: 07/01/2021

Importancia: Crítica

Recursos afectados:

RT430, RT431 & RT434, todas las versiones de firmware anteriores a la 08A06.

Descripción:

Tom Westenberg, de Thales UK, ha reportado estas vulnerabilidades a GE, que podrían permitir a un atacante remoto, autenticado, ejecutar código arbitrario en el sistema o interceptar y descifrar el tráfico encriptado.

Solución:

- Actualizar a la versión de firmware 08A06 o superior.

Las siguientes medidas de mitigación no garantizan una seguridad completa, pero deben considerarse hasta que se actualice el producto afectado:

- Utilizar una protección fuerte de seguridad física y de red para evitar que un atacante llegue a la red local donde normalmente se instalan los Reason RT43X.
- Bloquear los puertos TCP/IP 80 y 443 para bloquear el acceso HTTP/HTTPS a la interfaz web con los productos Reason RT43X, evitando todas las vulnerabilidades. Este bloqueo del puerto TCP/IP debe limitarse a la interfaz del puerto Ethernet donde Reason RT43X está conectado (por ejemplo, usando la lista de control de acceso (ACL)). De lo contrario, otras aplicaciones HTTP/HTTPS pueden verse afectadas.
- Minimizar la exposición a la red de todos los dispositivos y/o subsistemas del sistema de control y asegurarse de que no sean accesibles desde Internet.
- Analizar los eventos de seguridad para detectar a tiempo el tráfico/comunicación inesperado.

Detalle:

- Una vulnerabilidad de inyección de código en una de las páginas web, podría permitir a un atacante remoto, autenticado, ejecutar código arbitrario en el sistema. Se ha asignado el identificador CVE-2020-25197 para esta vulnerabilidad.
- Un atacante, con acceso a la clave criptográfica codificada, podría interceptar y descifrar el tráfico cifrado a través de una conexión HTTPS. Se ha asignado el identificador CVE-2020-25193 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Lectura fuera de límites en Panasonic FPWIN Pro

Fecha de publicación: 07/01/2021

Importancia: Alta

Recursos afectados:

- FPWIN Pro, versiones 7.5.0.0 y anteriores.

Descripción:

El investigador, Francis Provencher, junto con Trend Micro Zero Day Initiative, han comunicado al CISA una vulnerabilidad de severidad alta de tipo lectura fuera de límites.

Solución:

Actualizar a la versión 7.5.1.0.

Detalle:

Un atacante remoto podría ejecutar código arbitrario, después de que un usuario abriese un archivo de proyecto especialmente diseñado. Se ha asignado el identificador CVE-2020-16236 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Red Lion Crimson

Fecha de publicación: 07/01/2021

Importancia: Alta

Recursos afectados:

- Crimson 3.1, todas las versiones anteriores a la 3119.001.

Descripción:

Los investigadores, Marco Balduzzi, Ryan Flores, Philippe Lin, Charles Perine y Rainer Vosseler, junto con Trend Micro Zero Day Initiative, han informado al CISA de una vulnerabilidad, de severidad alta, de tipo referencia a puntero nulo y dos, de severidad media, de tipo ausencia de autenticación y fuga de memoria.

Solución:

Actualizar a la versión 3119.001 o posterior.

Detalle:

- Un atacante podría reiniciar el dispositivo mediante el envío de un paquete especialmente diseñado. Se ha asignado el identificador CVE-2020-27279 para esta vulnerabilidad.

- La configuración predeterminada podría permitir a un atacante leer o modificar la base de datos sin necesidad de autenticarse. Se ha asignado el identificador CVE-2020-27285 para esta vulnerabilidad.
- La liberación inadecuada de recursos podría permitir a un atacante provocar fugas de memoria arbitrarias, mediante el envío de mensajes especialmente diseñados. Se ha asignado el identificador CVE-2020-27283 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en Delta Electronics DOPSoft

Fecha de publicación: 07/01/2021

Importancia: Alta

Recursos afectados:

- DOPSoft, versiones 4.0.8.21 y anteriores.

Descripción:

Kimiya, trabajando con la iniciativa Zero Day de Trend Micro, ha informado al CISA de dos vulnerabilidades, de severidad alta, que podrían permitir a un atacante la ejecución arbitraria de código.

Solución:

- Actualizar a la versión 4.00.10.17 o superior.
- Utilizar DOPSoft v4.00.10.17 para abrir archivos de proyecto antiguos (*.dpa) y luego guardarlos como archivos nuevos, después eliminar los archivos antiguos.
- Limitar la interacción de la aplicación solo a archivos confiables.

Detalle:

Las vulnerabilidades de escritura fuera de límites o de referencia a un puntero nulo, podrían permitir a un atacante ejecutar código arbitrario, mientras se procesan archivos de proyecto. Se han asignado los identificadores CVE-2020-27275 y CVE-2020-27277 para estas vulnerabilidades.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Denegación de servicio en RSLinx Classic de Rockwell Automation

Fecha de publicación: 08/01/2021

Importancia: Alta

Recursos afectados:

RSLinx Classic 2.57.00.14 CPR 9 SR 3.

Descripción:

Se ha publicado una vulnerabilidad en la funcionalidad del servidor Ethernet/IP que podría permitir a un atacante la denegación de servicio.

Solución:

Por el momento no se ha aportado ninguna solución.

Detalle:

Una vulnerabilidad en la funcionalidad del servidor Ethernet/IP podría permitir a un atacante provocar la denegación de servicio mediante el envío de una solicitud de red especialmente elaborada. Se ha asignado el identificador CVE-2020-13573 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Vulnerabilidad en EASYsoft de Eaton

Fecha de publicación: 08/01/2021

Importancia: Media

Recursos afectados:

EASYsoft, versiones 7.20 y anteriores.

Descripción:

Francis Provencher, junto con Trend Micro's Zero Day Initiative, han reportado esta vulnerabilidad al CISA que podría permitir a un atacante local modificar el programa o provocar el cierre inesperado.

Solución:

- Eaton está trabajando en la solución, que está prevista para finales de enero.
- Eaton recomienda a los afectados que utilicen sólo archivos .E70 creados a partir de una fuente totalmente fiable y, en caso de que la aplicación falle debido a la carga del archivo .E70, reiniciar la aplicación y no volver a cargar dicho archivo .E70.

Detalle:

El producto afectado permite que un puntero se lea desde un objeto de un archivo, lo que provoca una confusión de tipos. Se ha asignado el identificador CVE-2020-6656 para esta vulnerabilidad.

La lectura fuera de límites podría permitir a un atacante modificar o bloquear el programa. Se ha asignado el identificador CVE-2020-6655 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, Vulnerabilidad

Ejecución arbitraria de código en CNCSoft-B de Delta Electronics

Fecha de publicación: 08/01/2021

Importancia: Alta

Recursos afectados:

CNCSoft-B, versiones 1.0.0.2 y anteriores.

Descripción:

Kimiya, junto con Trend Micro's Zero Day Initiative, ha reportado múltiples vulnerabilidades al CISA, que podrían permitir a un atacante ejecutar código arbitrario.

Solución:

Actualizar a CNCSoft-B v1.0.0.3.

Detalle:

La escritura fuera de límites, la lectura fuera de límites, un problema de desreferencia del puntero *null* o un problema de confusión de tipo, mientras se procesan los archivos del proyecto, podría permitir a un atacante ejecutar código arbitrario. Se han asignado los identificadores CVE-2020-27287, CVE-2020-27291, CVE-2020-27289 y CVE-2020-27293 para estas vulnerabilidades.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en Vital Signs Monitor VC150 de Innokas Yhtymä Oy

Fecha de publicación: 08/01/2021

Importancia: Media

Recursos afectados:

- Monitor Vital Signs VC150, versiones anteriores a la 1.7.15.

Descripción:

Los investigadores, Julian Suleder, Nils Emmerich, Birk Kauer y Oliver Matula, de ERNW, han reportado dos vulnerabilidades, de severidad media, de tipo cross-site scripting (XSS) e inyección de código.

Solución:

- Actualizar a la versión 1.7.15b o posterior.
- Adicionalmente, el fabricante recomienda:
  - Segmentar la red utilizando VLAN y aislar los dispositivos con medidas de seguridad.
  - Implementar protecciones físicas para evitar accesos no autorizados a los dispositivos.
  - Fomentar la conciencia de seguridad del personal hospitalario.

Detalle:

- Un atacante podría inyectar secuencias arbitrarias de comandos web o HTML, a través del parámetro de nombre de

archivo, en ciertos puntos de la interfaz web administrativa. Se ha asignado el identificador CVE-2020-27262 para esta vulnerabilidad.
- Un atacante podría inyectar segmentos de mensajes HL7 v2.x a través de múltiples parámetros, haciendo uso de un lector de código de barras. Se ha asignado el identificador CVE-2020-27260 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Autenticación inadecuada en FOX615 de Hitachi ABB Power Grids

Fecha de publicación: 08/01/2021

Importancia: Crítica

Recursos afectados:

- FOX61xR1, usando CESM1/CESM2, todas las versiones anteriores a cesne_r1h07_12.esw;
- FOX61xR2, usando CESM1/CESM2, todas las versiones anteriores a cesne_r2d14_03.esw.

Descripción:

Hitachi ABB Power Grids ha reportado al CISA una vulnerabilidad, de severidad crítica, de tipo autenticación inadecuada.

Solución:

- FOX61xR1: actualizar a la versión cesne_r1h07_12.esw o posterior;
- FOX61xR2: actualizar a la versión cesne_r2d14_03.esw o posterior.

Detalle:

Un atacante podría enviar un mensaje, especialmente diseñado, para iniciar un canal de comunicación sin necesidad de autenticación y ejecutar comandos arbitrarios de forma remota. Se ha asignado el identificador CVE-2018-10933 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en CX-One de Omron

Fecha de publicación: 08/01/2021

Importancia: Alta

Recursos afectados:

- CX-One, versiones 4.60 y anteriores, incluyendo las siguientes aplicaciones:
  - CX-Protocol, versiones 2.02 y anteriores;
  - CX-Server, versiones 5.0.28 y anteriores;
  - CX-Position, versiones 2.52 y anteriores.

Descripción:

El investigador, rgod, trabajando con Zero Day Initiative de Trend Micro, ha informado al CISA de una vulnerabilidad, de severidad alta, de tipo desbordamiento de búfer y dos vulnerabilidades, de severidad media, de tipo ejecución remota de código.

Solución:

Actualizar a:

- CX-Protocol versión 2.03;
- CX-Server versión 5.0.29;
- CX-Position versión 2.53.

Detalle:

- Una vulnerabilidad de desbordamiento de búfer basado en pila (stack), podría permitir a un atacante la ejecución remota de código arbitrario. Se ha asignado el identificador CVE-2020-27261 para esta vulnerabilidad.
- Para el resto de vulnerabilidades se han asignado los identificadores CVE-2020-27259 y CVE-27257.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Avisos de seguridad de Siemens de enero de 2021

Fecha de publicación: 12/01/2021

Importancia: Crítica

Recursos afectados:

- SCALANCE X-200 (incluidas las variantes SIPLUS NET), todas las versiones;
- SCALANCE X-200IRT (incluidas las variantes SIPLUS NET), todas las versiones;
- SCALANCE X-300 (incluidas las variantes X408 y SIPLUS NET), versiones anteriores a la V4.1.0;
- JT2Go, versiones anteriores a la V13.1.0;
- Teamcenter Visualization, versión V13.1.0 y anteriores;
- Solid Edge, versiones anteriores a la SE2021MP2;

Descripción:

Siemens ha publicado en su comunicado mensual varias actualizaciones de seguridad de diferentes productos.

Solución:

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

Detalle:

Siemens, en su comunicación mensual de parches de seguridad, ha emitido un total de 12 avisos de seguridad, de los cuales 8 son actualizaciones.

Los tipos de nuevas vulnerabilidades publicadas se corresponden con los siguientes:

- 10 vulnerabilidades de escritura fuera de límites,
- 6 vulnerabilidades de desbordamiendo de búfer basado en pila (*Stack*),
- 5 vulnerabilidades de desbordamiento de búfer basado en memoria dinámica (*Heap*),
- 2 vulnerabilidades de acceso de recurso mediante un tipo incompatible (confusión de tipos),
- 2 vulnerabilidades de uso de clave criptográfica embebida,
- 1 vulnerabilidad de ausencia de autenticación en función crítica,
- 1 vulnerabilidad de ausencia de referencia a puntero no confiable,
- 1 vulnerabilidad de restricción incorrecta de referencia a entidad externa XML (*XXE*),
- 1 vulnerabilidad de lectura fuera de límites,

Para estas vulnerabilidades se han reservado los siguientes identificadores:

CVE-2020-15799, CVE-2020-15800, CVE-2020-25226, CVE-2020-28391, CVE-2020-28395, CVE-2020-26980, CVE-2020-26981, CVE-2020-26982, CVE-2020-26983, CVE-2020-26984, CVE-2020-26985, CVE-2020-26986, CVE-2020-26987, CVE-2020-26988, CVE-2020-26989, CVE-2020-26990, CVE-2020-26991, CVE-2020-26992, CVE-2020-26993, CVE-2020-26994, CVE-2020-26995, CVE-2020-26996, CVE-2020-28383, CVE-2020-28381, CVE-2020-28382, CVE-2020-28383, CVE-2020-28384, CVE-2020-28386 y CVE-2020-26989.

Etiquetas: Actualización, Infraestructuras críticas, Siemens, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Schneider Electric

Fecha de publicación: 13/01/2021

Importancia: Crítica

Recursos afectados:

- EcoStruxure Power Build - Rapsody, versiones 2.1.13 y anteriores;
- EcoStruxure™ Operator Terminal Expert 3.1 Service Pack 1A y anteriores, con Harmony HMIs:
  - Series HMIST6,
  - HMIG3U en series HMIGTU,
  - Series HMISTO.
- Pro-face BLUE 3.1 Service Pack 1A y anteriores, con Pro-face HMIs:
  - Series ST6000,
  - SP-5B41 en series SP5000,
  - Series GP4100.

Descripción:

Schneider Electric ha publicado tres vulnerabilidades, de severidad alta, que afecta a alguno de sus productos.

Solución:

- La solución para la vulnerabilidad en EcoStruxure Power Build - Rapsody, está prevista para el primer semestre de 2021, hasta ese momento el fabricante recomienda:
  - Aplicar el principio del menor privilegio para limitar el acceso a la computadora que ejecuta el software Rapsody.
  - Implementar una lista blanca de aplicaciones para bloquear la ejecución de código malicioso.
  - Instalar un antivirus en el ordenador y mantenerlo actualizado.
- Actualizar a EcoStruxure™ Operator Terminal Expert V3.1 Service Pack 1B;
- Actualizar a Pro-face BLUE V3.1 Service Pack 1B;

Detalle:

- Cuando se sube un archivo SSD malicioso y se analiza inadecuadamente, un atacante podría causar una condición de uso de la memoria previamente liberada (*use-after-free*) o un desbordamiento del búfer basado en la pila (*stack*) que resultaría en la ejecución de código remoto. Se han asignado los identificadores CVE-2021-22697 y CVE-2021-22698

para esta vulnerabilidad.
- Una vulnerabilidad de validación de entrada inapropiada podría permitir a un atacante la ejecución de código arbitrario cuando la función *Ethernet Download* está habilitada en el HMI. Se ha asignado el identificador CVE-2020-28221 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Schneider Electric, Vulnerabilidad

---

Múltiples vulnerabilidades en productos SOOIL

Fecha de publicación: 13/01/2021

Importancia: Alta

Recursos afectados:

- Dana Diabecare RS, todas las versiones anteriores a la 3.0;
- AnyDana-i, todas las versiones anteriores a la 3.0;
- AnyDana-A, todas las versiones anteriores a la 3.0.

Descripción:

Los investigadores Julian Suleder, Birk Kauer, Raphael Pavlidis y Nils Emmerich, de ERNW Research GmbH, han reportado a la Oficina Federal para la Seguridad de la Información (BSI) una vulnerabilidad de severidad alta de tipo claves deterministas y 8 vulnerabilidades de severidad media.

Solución:

- Actualizar:
  - Dana Diabecare RS a la versión 3.0, posterior o última disponible.
  - AnyDana-i y AnyDana-A a la versión 3.0 o posterior.
- Adicionalmente, el fabricante recomienda que, en caso de no poder actualizar Dana RS, operar esta siempre en Airplane Mode.

Detalle:

Un atacante, próximo físicamente y no autenticado, podría realizar un ataque de fuerza bruta a través de Bluetooth Low Energy, aprovechando las claves deterministas que utiliza el protocolo de comunicación. Se ha asignado el identificador CVE-2020-27264 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores CVE-2020-27256, CVE-2020-27258, CVE-2020-27266, CVE-2020-27268, CVE-2020-27269, CVE-2020-27270, CVE-2020-27272 y CVE-2020-27276.

Etiquetas: Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

---

Vulnerabilidad en fdtContainer de WAGO/M&M Software

Fecha de publicación: 15/01/2021

Importancia: Alta

Recursos afectados:

- fdtCONTAINER component:
  - versiones anteriores a la 3.5;
  - versiones 3.5.0, anteriores a la 3.5.20304.x;
  - versiones 3.6.0, anteriores a la 3.6.20304.x;
- fdtCONTAINER application:
  - versiones anteriores a la 4.5;
  - versiones 4.5.0, anteriores a la 4.5.20304.x;
  - versiones 4.6.0, anteriores a la 4.6.20304.x;
- dtmINSPECTOR:
  - versión 3 (basada en FDT 1.2.x).

Descripción:

Un cliente de *fdtCONTAINER component* ha reportado esta vulnerabilidad de severidad alta, coordinada por , que podría permitir a un atacante ejecutar código malicioso.

Solución:

El fabricante aporta 2 soluciones posibles:

- Por un lado, actualizar a una versión que proporcione una deserialización más segura de los datos del proyecto. Estas versiones seguirán utilizando una tecnología de serialización obsoleta, pero corregirá el vector de ataque actualmente conocido y será compatible con los archivos de proyecto existentes, no manipulados:
  - fdtCONTAINER component, versión 3.6.20304.x o superior;
  - fdtCONTAINER application, versión 4.6.20304.x o superior.
- Por otro, actualizar a una versión que proporciona una deserialización segura de los datos del proyecto con una tecnología de serialización actualizada. Esto provoca la incompatibilidad con los archivos de proyecto existentes, no

manipulados:
- fdtCONTAINER component, versión 3.7 y superiores;
- fdtCONTAINER application, versión 4.7 y superiores.

Detalle:

Una vulnerabilidad de deserialización de datos no confiables podría permitir a un atacante ejecutar código malicioso, desde la estación de trabajo en la que se ejecuta la aplicación del host, con los permisos de usuario de dicha aplicación. Se ha asignado el identificador CVE-2020-12525 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad en Dnsmasq en Sistemas de Control Industrial

Fecha de publicación: 20/01/2021

Importancia: Alta

Recursos afectados:

- Dnsmasq DNS y servidor DHCP, versión 2.8.2 y anteriores.

Varios fabricantes de productos de Sistemas de Control Industrial se han visto afectados por esta vulnerabilidad en Dnsmasq, para conocer el listado completo de productos afectados, consulte la sección de referencias.

Descripción:

Múltiples vulnerabilidades en la implementación de la DNSSEC dnsmasq podrían permitir a un atacante remoto, no autenticado, envenenar la caché, divulgar información, ejecutar código arbitrario o causar una condición de denegación de servicio (DoS) en un dispositivo afectado. Las vulnerabilidades se agrupan y se denominan DNSpooq.

Solución:

- Actualizar a dnsmasq 2.83.
- Se recomiendan las siguientes medidas de mitigación:
  - Implementar las características de seguridad de la capa 2, como el DHCP snooping y la protección de la fuente IP.
  - Configurar Dnsmasq para que no escuche las interfaces WAN si no es necesario.
  - Reducir el máximo de consultas permitidas para ser reenviadas con la opción --dns-forward-max=< consultas >. El valor por defecto es 150, pero podría reducirse.
  - Deshabilitar temporalmente la opción de validación de DNSSEC hasta que se actualice.
  - Utilizar DNS-over-HTTPS o DNS-over-TLS para conectarse al servidor upstream.
- Para conocer las medidas propias de cada fabricante, consulte la sección de referencias.

Detalle:

- Una vulnerabilidad de desbordamiento de búfer basado en memoria dinámica (*Heap*) debida a la ordenación de los RRSets antes de validarlos con los datos de DNSSEC, podría permitir a un atacante ejecutar código arbitrario mediante el envío de una respuesta DNS especialmente diseñada. Se ha asignado el identificador CVE-2020-25681 para esta vulnerabilidad.
- Una vulnerabilidad de desbordamiento de búfer basado en memoria dinámica (*Heap*) debida a la extracción de nombres de paquetes DNS antes de validarlos con los datos de DNSSEC, podría permitir a un atacante ejecutar código arbitrario mediante el envío de una respuesta DNS especialmente diseñada. Se ha asignado el identificador CVE-2020-25682 para esta vulnerabilidad.
- Las vulnerabilidades de desbordamiento de búfer basado en memoria dinámica (*Heap*) cuando DNSSEC está activado, antes de validar las entradas recibidas, podría permitir a un atacante denegar el servicio mediante el envío de respuestas DNS válidas. Se ha asignado el identificador CVE-2020-25683 y CVE-2020-25687 para estas vulnerabilidades.
- La validación insuficiente de la autenticidad de los datos en la respuesta de una consulta reenviada cuando Dnsmasq comprueba en forward.c:reply_query() si la dirección / puerto de destino de la respuesta, es utilizada por las consultas reenviadas pendientes, podría permitir a un atacante realizar un ataque de envenenamiento de la caché del DNS. Se ha asignado el identificador CVE-2020-25684 para esta vulnerabilidad.
- El uso de un algoritmo criptográfico roto o débil podría permitir a un atacante encontrar varios dominios diferentes con el mismo hash fuera de ruta, reduciendo considerablemente el número de intentos de falsificar una respuesta para su aceptación por parte de Dnsmasq, y realizar un ataque de envenenamiento de la caché del DNS. Se ha asignado el identificador CVE-2020-25685 para esta vulnerabilidad.
- La validación insuficiente de la autenticidad de los datos, al recibir una consulta en la que Dnsmasq no comprueba si existe una solicitud pendiente con el mismo nombre antes de reenviar una nueva solicitud, podría permitir a un atacante, fuera de la ruta de la red, reducir considerablemente el número de intentos de falsificar una respuesta para su aceptación por parte de Dnsmasq, y realizar un ataque de envenenamiento de la caché del DNS. Se ha asignado el identificador CVE-2020-25686 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, DNS, Infraestructuras críticas, Siemens, Vulnerabilidad

---

Múltiples vulnerabilidades en productos P2P de Reolink

Fecha de publicación: 20/01/2021

Importancia: Crítica

Recursos afectados:

Todos los productos de las series:

- RLC-4XX;
- RLC-5XX;
- RLN-X10.

Descripción:

Nozomi Networks ha reportado al CISA dos vulnerabilidades, una de severidad crítica y otra de severidad alta, que podrían permitir a un atacante acceder a información confidencial o comprometer los equipos fuera de la red local.

Solución:

Se recomienda desactivar la función P2P en los dispositivos Reolink y actualizar el firmware de los mismos.

Detalle:

- Un atacante con acceso a la red local podría obtener una clave de cifrado fija que le permitiría comprometer las cámaras P2P Reolink fuera de esta red. Se ha asignado el identificador CVE-2020-25173 para esta vulnerabilidad.
- La falta de seguridad en el protocolo P2P, para la transferencia de datos entre el dispositivo local y los servidores de Reolink, podría permitir a un atacante acceder a información confidencial. Se ha asignado el identificador CVE-2020-25169 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Neutralización incorrecta de elementos especiales en estaciones de trabajo de Philips

Fecha de publicación: 20/01/2021

Importancia: Media

Recursos afectados:

Estaciones de trabajo de identificación 12NC correspondiente a:

- 4598 009 39471;
- 4598 009 39481;
- 4598 009 70861;
- 4598 009 98531;

que ejecuten el siguiente *software*:

- Interventional Workspot, versiones 1.3.2, 1.4.0, 1.4.1, 1.4.3 y 1.4.5;
- Coronary Tools, version 1.0;
- Dynamic Coronary Roadmap, version 1.0;
- Stentboost Live, versión 1.0;
- ViewForum, version 6.3V1L10.

Descripción:

Philips ha reportado al CISA una vulnerabilidad de severidad media que podría permitir a un atacante, dentro de la red, apagar o reiniciar, de forma remota, una de las estaciones de trabajo.

Solución:

- Philips ha publicado un parche para abordar de forma proactiva esta vulnerabilidad y programará actividades de soporte con los clientes afectados para implementar la corrección.
- Como medidas de mitigación, el fabricante recomienda cambiar la contraseña de IPMI para la interfaz de la estación de trabajo.

Detalle:

La neutralización inadecuada de elementos especiales, utilizados en comandos del sistema operativo, podría permitir a un atacante modificar dichos comandos al ser enviados a otro componente. Se ha asignado el identificador CVE-2020-27298 para esta vulnerabilidad.

Etiquetas: Actualización, Sanidad

Múltiples vulnerabilidades en Bosch Fire Monitoring System

Fecha de publicación: 21/01/2021

Importancia: Crítica

Recursos afectados:

- Bosch FSM-2500, versiones 5.2 y anteriores;
- Bosch FSM-5000, versiones 5.2 y anteriores.

Descripción:

Durante la realización de pruebas internas del producto, Bosch detectó 2 vulnerabilidades, con severidad crítica y media, que afectan a las versiones 5.2 y anteriores de FSM (*Fire Monitoring System*).

Solución:

Actualizar FSM a las versiones 5.6 o superiores.

Detalle:

- El uso de credenciales embebidas en la base de datos podría permitir a un atacante remoto, no autenticado, loguearse en la base de datos con privilegios de administrador. Esto podría dar lugar a un compromiso total de la confidencialidad e integridad de los datos almacenados, así como a un impacto de alta disponibilidad en la propia base de datos. Además, el atacante también podría ejecutar comandos arbitrarios en el sistema operativo subyacente. Se ha asignado el identificador CVE-2020-6779 para la vulnerabilidad con severidad crítica.
- La utilización de credenciales poco seguras en la base de datos podría permitir a un atacante remoto, con privilegios de administrador, obtener las credenciales de otros usuarios y recuperar sus contraseñas en texto plano mediante ataques fuerza bruta del *hash* MD5. Se ha asignado el identificador CVE-2020-6780 para la vulnerabilidad con severidad media.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad de denegación de servicio en AC500 V2 de ABB

Fecha de publicación: 21/01/2021

Importancia: Alta

Recursos afectados:

Todos los productos AC500 V2 con interfaz ethernet.

Descripción:

ABB ha informado de una vulnerabilidad en AC500 V2 que permitiría a un atacante causar una denegación de servicio. Después del bloqueo del dispositivo (ERR LED parpadea en rojo) se requiere un reinicio físico del dispositivo.

Solución:

ABB ha publicado el *firmware* versión 2.8.5 que corrige esta vulnerabilidad en los siguientes modelos de PLC:

- PM573-ETH
- PM583-ETH

Para otros modelos de PLC afectados, ABB recomienda hasta la publicación de un nuevo *firmware* y limitar la exposición a través de redes no confiables o públicas.

Detalle:

ABB ha informado de una vulnerabilidad que permitiría a un atacante, a través del envío de un paquete manipulado y no autenticado, causar una denegación de servicio en los PLC afectados, requiriendo después del bloqueo (ERR LED parpadea en rojo) un reinicio físico del mismo. Se ha asignado el identificador CVE-2020-24685 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Infraestructuras críticas, SCADA, Vulnerabilidad

---

Múltiples vulnerabilidades en varios productos de Delta Electronics

Fecha de publicación: 22/01/2021

Importancia: Alta

Recursos afectados:

- ISPSoft, versión 3.12 y anteriores;
- TPEditor, versión 1.98 y anteriores.

Descripción:

Los investigadores de seguridad, Francis Provencher y *kimiya*, en colaboración con ZDI de Trend Micro, han reportado 3

vulnerabilidades, todas de severidad alta, que permitirían a un atacante ejecutar código bajo los privilegios de la aplicación.

Solución:

- Actualizar ISPSoft a la versión 3.12.01;
- actualizar TPEditor a la versión 1.98.03.

Detalle:

- Se ha identificado un problema de uso de memoria previamente liberada (*use after free*) en el procesado de los archivos de proyecto que podría permitir a un atacante crear un archivo de proyecto, especialmente diseñado, para realizar una ejecución de código arbitrario. Se ha asignado el identificador CVE-2020-27280 para esta vulnerabilidad.
- Se ha detectado una desreferencia de puntero no confiable en el procesado de los archivos de proyecto que podría permitir a un atacante crear un archivo de proyecto, especialmente diseñado, para realizar una ejecución de código arbitrario. Se ha asignado el identificador CVE-2020-27288 para esta vulnerabilidad.
- El producto afectado es vulnerable a dos instancias de escritura fuera de límites en el procesado de los archivos de proyecto, lo que podría permitir a un atacante crear un archivo de proyecto, especialmente diseñado, para realizar una ejecución de código arbitrario. Se ha asignado el identificador CVE-2020-27284 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en OPC UA Tunneller de Matrikon

Fecha de publicación: 22/01/2021

Importancia: Crítica

Recursos afectados:

OPC UA Tunneller, todas las versiones anteriores a 6.3.0.8233.

Descripción:

El investigador, Uri Katz de Claroty, ha descubierto varias vulnerabilidades en OPC UA Tunneller de Matrikon, una marca de Honeywell. Estas vulnerabilidades permitirán a un atacante remoto acceder a información confidencial, ejecutar código arbitrario de forma remota o bloquear el dispositivo y causar una denegación de servicio.

Solución:

Honeywell recomienda actualizar Matrikon OPC UA Tunneller a la versión 6.3.0.8233.

Detalle:

La vulnerabilidad más importante descubierta en OPC UA Tunneller permitiría la ejecución remota de código arbitrario a través de un desbordamiento de búfer basado en *heap*, manipulando los valores en memoria y causando la ejecución de código arbitrario. Se ha asignado el identificador CVE-2020-27297 para esta vulnerabilidad crítica.

Otras vulnerabilidades detectadas se corresponden con los siguientes identificadores: CVE-2020-27299, CVE-2020-27274 y CVE-2020-27295.

Etiquetas: Actualización, Infraestructuras críticas, SCADA, Vulnerabilidad

---

Consumo incontrolado de recursos en controladores MELFA de Mitsubishi Electric

Fecha de publicación: 22/01/2021

Importancia: Alta

Recursos afectados:

- Controladores de robot MELFA serie FR:
  - RV-#FR$%/ CR800-#V$D;
  - RH-#FRH$&/ CR800-#HD;
  - RH-#FRHR$&/ CR800-#HRD;
  - RV-#FR$%/ R16RTCPU CR800-#V$R;
  - RH-#FRH$&/ R16RTCPU CR800-#HR;
  - RH-#FRHR$&/ R16RTCPU CR800-#HRR;
  - RV-#FR$%/ Q172DSRCPU CR800-#V$Q;
  - RH-#FRH$&/ Q172DSRCPU CR800-#HQ;
  - RH-#FRHR$&/ Q172DSRCPU CR800-#HRQ.
- Controladores de robot MELFA serie CR:
  - CR800-CVD;
  - RH-# CR800-CHD.
- Controlador de robot MELFA serie ASSISTA: CR800-05VD.

Descripción:

Industrial Control Security Laboratory, de Qi An Xin Group, ha reportado a Mitsubishi Electric una vulnerabilidad, de severidad alta, por la que un atacante podría provocar una condición de denegación de servicio.

Solución:

Verificar la versión de *firmware* de acuerdo al sitio web de Mitsubishi Electric.

Adicionalmente, Mitsubishi Electric recomienda tomar las siguientes medidas de mitigación:

- Utilizar un firewall o una VPN para evitar el acceso no autorizado cuando se requiera acceso a Internet.
- Usar el dispositivo dentro de una LAN, bloqueando el acceso a esta desde redes y host no fiables mediante *firewalls*.

Para obtener información adicional sobre la vulnerabilidad y soluciones, póngase en contacto con un representante de Mitsubishi Electric.

Detalle:

Una vulnerabilidad de consumo incontrolado de recursos podría permitir a un atacante provocar una condición de denegación de servicio en la ejecución del programa robot o en la comunicación Ethernet, mediante el envío de una gran cantidad de paquetes en poco tiempo. Se ha asignado el identificador CVE-2021-20586 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en productos Fuji Electric

Fecha de publicación: 27/01/2021

Importancia: Alta

Recursos afectados:

- Tellus Lite V-Simulator, versiones anteriores a la v4.0.10.0;
- V-Server Lite, versiones anteriores a la v4.0.10.0.

Descripción:

Se han publicado múltiples vulnerabilidades en productos de Fuji Electric que podrían permitir a un atacante ejecutar código con los mismos privilegios que la aplicación.

Solución:

Actualizar a la versión v4.0.10.0:

- v4.0.10.0 Disk 1;
- v4.0.10.0 Disk 2.

Detalle:

La forma en la que la aplicación procesa los archivos de proyecto podría permitir a un atacante crear un archivo de proyecto, especialmente diseñado, para ejecutar código arbitrario, aprovechando alguna de las siguientes vulnerabilidades:

- Desbordamiento de búfer basado en pila (*stack*). Se ha asignado el identificador CVE-2021-22637 para esta vulnerabilidad.
- Lectura fuera de límites. Se ha asignado el identificador CVE-2021-22655 para esta vulnerabilidad.
- Escritura fuera de límites. Se ha asignado el identificador CVE-2021-22653 para esta vulnerabilidad.
- Puntero no inicializado. Se ha asignado el identificador CVE-2021-22639 para esta vulnerabilidad.
- Desbordamiento de búfer basado en memoria dinámica (*heap*). Se ha asignado el identificador CVE-2021-22641 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Autenticación inapropiada en 4CCT

Fecha de publicación: 28/01/2021

Importancia: Alta

Recursos afectados:

4CCT-EA6-334126BF, versión de *firmware* 3.23.77.8.33251.

Descripción:

INCIBE ha coordinado la publicación de una vulnerabilidad en el dispositivo ZIV 4CCT, con el código interno INCIBE-2021-0040, que ha sido descubierto por Aarón Flecha Menéndez.

Se ha asignado el código CVE-2021-25910 para esta vulnerabilidad. Se ha calculado una puntuación base de 7.6 según CVSS v3; siendo el cálculo del CVSS el siguiente: AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:H/AR:M/MAV:A/MAC:L/MPR:X/MUI:R/MS:U/MC:H/MI:H/MA:H.

Solución:

Actualizar a la versión 3.23.80.58.46120.

Esta situación también puede evitarse forzando el acceso HTTPS o limitando los accesos locales físicos a los dispositivos.

Detalle:

Un uso incorrecto del parámetro *cookie* en el dispositivo 4CCT, de ZIV Automation, permite a un atacante realizar modificaciones en varios parámetros del dispositivo afectado como usuario autenticado.

La vulnerabilidad se debe a un uso incorrecto del parámetro *cookie,* ya que no dispone de todos los mecanismos de seguridad necesarios para evitar un secuestro de sesión.

Para explotar la vulnerabilidad, el atacante debe estar dentro de la red donde se encuentra el dispositivo afectado.

CWE-287: Autenticación incorrecta.

Línea temporal:
04/07/2020 ? Descubrimiento de los investigadores.
17/08/2020 ? Investigadores contactan con INCIBE.
30/10/2020 ? El fabricante confirma la vulnerabilidad a INCIBE.
21/12/2020 ? ZIV confirma que la versión *fix* y la nueva versión *software* han sido publicadas (*Security Patch/new version*).
28/01/20201 ? El aviso es publicado por INCIBE.

Si tiene más información sobre este aviso, póngase en contacto con INCIBE, como se indica en el reporte de vulnerabilidades al CNA.

Etiquetas: 0day, Actualización, CNA, Vulnerabilidad

Denegación de servicio en 4CCT

Fecha de publicación: 28/01/2021

Importancia: Alta

Recursos afectados:

4CCT-EA6-334126BF, versión de *firmware* 3.23.80.27.36371.

Descripción:

INCIBE ha coordinado la publicación de una vulnerabilidad en el dispositivo ZIV 4CCT, con el código interno INCIBE-2021-0039, que ha sido descubierto por Aarón Flecha Menéndez.

Se ha asignado el código CVE-2021-25909 para esta vulnerabilidad. Se ha calculado una puntuación base de 8.2 según CVSS v3; siendo el cálculo del CVSS el siguiente: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:H/RL:O/RC:C/CR:X/IR:X/AR:M/MAV:N/MAC:X/MPR:X/MUI:N/MS:C/MC:N/MI:N/MA:H.

Solución:

Actualizar a la versión 3.23.80.58.46120.

Esta situación también puede evitarse instalando el dispositivo en una red con el ancho de banda limitado y con requisito de privilegios de acceso.

Detalle:

El dispositivo 4CCT, de ZIV Automation, es vulnerable a ataques de denegación de servicio a través del puerto 7919.

La explotación de esta vulnerabilidad podría permitir a un atacante remoto causar una interrupción en el funcionamiento del dispositivo mediante el envío de paquetes específicos al puerto 7919.

Una vez finalizado el ataque, el dispositivo recupera gradualmente su funcionamiento normal.

CWE-400: Consumo de recursos no controlado (Agotamiento de recursos).

Línea temporal:

10/03/2020 ? Descubrimiento de los investigadores.
25/05/2020 ? Investigadores contactan con INCIBE.
03/07/2020 ? El fabricante confirma la vulnerabilidad a INCIBE.
21/12/2020 ? ZIV confirma que la versión *fix* y la nueva versión *software* han sido publicadas (*Security Patch/new version*).
28/01/2021 ? El aviso es publicado por INCIBE.

Si tiene más información sobre este aviso, póngase en contacto con INCIBE, como se indica en el reporte de vulnerabilidades al CNA.

Etiquetas: 0day, Actualización, CNA, Vulnerabilidad

Vulnerabilidad en paneles SIMATIC HMI de Siemens

Fecha de publicación: 29/01/2021

Importancia: Alta

Recursos afectados:

- SIMATIC HMI Comfort Panels (incluidas las variantes SIPLUS), todas las versiones anteriores a la V16 Update 3a;
- SIMATIC HMI KTP Mobile Panels, todas las versiones anteriores a la V16 Update 3a.

Descripción:

Los paneles SIMATIC HMI están afectados por una vulnerabilidad que podría permitir a un atacante remoto obtener acceso completo al dispositivo, si el servicio telnet está habilitado.

Solución:

Actualizar a las versiones:

- SIMATIC HMI Comfort Panels V16 Update 3a o superior;
- SIMATIC HMI KTP Mobile Panels V16 Update 3a o superior.

Para reducir el riesgo, Siemes recomienda desactivar telnet en los paneles HMI, si está activado (desactivado por defecto).

Detalle:

Los dispositivos afectados, con el servicio telnet activado, no requieren ninguna autenticación para este servicio, por lo que un atacante remoto podría obtener acceso completo al dispositivo. Se ha asignado el identificador CVE-2020-15798 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Siemens, Vulnerabilidad