Boletín de marzo de 2021

Avisos de Sistemas de Control Industrial

Vulnerabilidad en fdtContainer afecta a múltiples productos de ENDRESS HAUSER

Fecha de publicación: 01/03/2021

Importancia: Alta

Recursos afectados:

- DeviceCare SFE100, versión 1.07.00 y anteriores;
- Field Xpert SMTxx (Software SFE300), versión 1.05.00 y anteriores;
- FieldCare SFE500, versión 2.15.01 y anteriores;
- Asset Health Monitoring SRP700 (Software FieldCare SFE500), versión 2.15.01 (FieldCare SFE500) y anteriores.

Descripción:

M&M Software GmbH ha reportado esta vulnerabilidad de severidad alta, coordinada por , que podría permitir a un atacante ejecutar código malicioso.

Solución:

Hasta que esté disponible una solución, se recomienda tomar las siguientes medidas de mitigación:

- intercambiar los datos del proyecto sólo a través de servicios de intercambio seguros;
- utilizar los medios adecuados para proteger el almacenamiento del proyecto de manipulaciones no autorizadas;
- no abrir los datos del proyecto desde una fuente desconocida;
- reducir los derechos de usuario de la aplicación anfitriona al mínimo necesario.

Detalle:

Una vulnerabilidad de deserialización de datos no confiables en el componente fdtContainer, integrado en la aplicación, 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 ya publicada en INCIBE-CERT.

Etiquetas: Infraestructuras críticas, Vulnerabilidad

Validación de entrada incorrecta en múltiples productos de Rockwell Automation

Fecha de publicación: 03/03/2021

Importancia: Media

Recursos afectados:

Las siguientes versiones de dispositivos de Rockwell Automation están afectadas:

- controladores Armor Compact GuardLogix 5370, versiones 33 y anteriores;
- controladores de seguridad Armor GuardLogix, versiones 33 y anteriores;
- controladores CompactLogix 5370 L1, versiones 33 y anteriores;

- controladores CompactLogix 5370 L2s, versiones 33 y anteriores;
- controladores CompactLogix 5370 L3, versiones 33 y anteriores;
- controladores Compact GuardLogix 5370, versiones 33 y anteriores;
- controladores ControlLogix 5570, versiones 33 y anteriores.

Descripción:

El investigador, Yeop Chang, ha reportado una vulnerabilidad, de severidad media, de tipo validación de entrada incorrecta, que podría afectar a múltiples controladores de Rockwell Automation,

Solución:

Rockwell Automation recomienda a los usuarios afectados que actualicen el *firmware* a la versión 33.011 o posterior.

Detalle:

El algoritmo para establecer la conexión, utilizado por CompactLogix 5370 y ControlLogix 5570, no gestiona correctamente su flujo de control durante la ejecución, creando un bucle infinito. Esto podría permitir a un atacante enviar solicitudes de paquetes CIP (*Common Industrial Protocol*), especialmente diseñados, a un controlador, provocando condiciones de denegación de servicio en las comunicaciones con otros productos. Se ha asignado el identificador CVE-2020-6998 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en Ellipse EAM de Hitachi ABB Power Grids

Fecha de publicación: 03/03/2021

Importancia: Media

Recursos afectados:

Ellipse Enterprise Asset Management (EAM), versión 9.0.25 y anteriores.

Descripción:

Hitachi ABB Power Grids ha reportado al CISA dos vulnerabilidades de severidad media que podrían permitir a un atacante robar información confidencial, secuestrar la sesión del usuario o comprometer credenciales de autenticación.

Solución:

Actualizar a la versión 9.0.26.

Detalle:

- Una vulnerabilidad de XSS (*Cross Site Scripting*) podría permitir a un atacante engañar a un usuario para que acceda a un vínculo que contiene código malicioso, el cual se ejecutaría en el navegador web, con lo que el atacante podría comprometer información confidencial o secuestrar la sesión del usuario. Se ha asignado el identificador CVE-2021-27416 para esta vulnerabilidad.
- Una vulnerabilidad de *clickjacking* podría permitir a un atacante engañar a un usuario para que visite un sitio web que se haga pasar por una interfaz de inicio de sesión de la aplicación Ellipse y así, comprometer las credenciales de autenticación del usuario. Se ha asignado el identificador CVE- 2021-27414 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad de canal lateral en múltiples productos Bosch

Fecha de publicación: 04/03/2021

Importancia: Media

Recursos afectados:

- Bosch AUTODOME 700 IP IVA en: CPP3;
- Bosch AUTODOME 7000 series en: CPP4;
- Bosch AUTODOME 800 en: CPP3;
- Bosch AUTODOME Easy II IP series en: CPP3;
- Bosch AUTODOME IP 4000 HD en: CPP4;
- Bosch AUTODOME IP 4000i en: CPP7.3;
- Bosch AUTODOME IP 5000 HD en: CPP4;
- Bosch AUTODOME IP 5000 IR en: CPP4;
- Bosch AUTODOME IP 5000i en: CPP7.3;
- Bosch AUTODOME IP starlight 5000i (IR) en: CPP7.3;
- Bosch AUTODOME IP starlight 7000i en: CPP7.3;
- Bosch AUTODOME Junior 800 en: CPP3;
- Bosch AUTODOME Junior HD, Jr HD fix en: CPP3;
- Bosch DINION 2X, NBN-498-P en: CPP3;

- Bosch DINION HD 1080p en: CPP4;
- Bosch DINION HD 1080p HDR en: CPP4;
- Bosch DINION HD 720p en: CPP4;
- Bosch DINION IP 3000i en: CPP7.3;
- Bosch DINION IP 4000 HD en: CPP4;
- Bosch DINION IP 5000 HD en: CPP4;
- Bosch DINION IP 5000 MP en: CPP4;
- Bosch DINION IP bullet 4000 en: CPP4;
- Bosch DINION IP bullet 4000i en: CPP7.3;
- Bosch DINION IP bullet 5000 en: CPP7.3;
- Bosch DINION IP bullet 5000 en: CPP4;
- Bosch DINION IP bullet 5000i en: CPP7.3;
- Bosch DINION IP bullet 6000i en: CPP7.3;
- Bosch DINION IP starlight 6000 en: CPP7;
- Bosch DINION IP starlight 7000 en: CPP7;
- Bosch DINION IP starlight 7000 HD en: CPP4;
- Bosch DINION IP starlight 8000 12MP en: CPP6;
- Bosch DINION IP thermal 8000 en: CPP7;
- Bosch DINION IP thermal 9000 RM en: CPP7;
- Bosch DINION IP ultra 8000 12MP en: CPP6;
- Bosch DINION IP ultra 8000 12MP con teleobjetivo con montura C/CS en: CPP6;
- Bosch DINION XF 720p , NBN-921-P en: CPP3;
- Bosch DINION XF, NBC-455-P en: CPP3;
- Bosch DINION imager 9000 HD en: CPP4;
- Bosch EXTEGRA IP dynamic 9000 en: CPP4;
- Bosch EXTEGRA IP starlight 9000 en: CPP4;
- Bosch Economic versión VIP-X1XF-E en: CPP3;
- Bosch Economy Box Cameras, NBC-225 series, NBC-255 series, NTC-255-PI en: CPP3;
- Bosch Economy Dome Cameras, NDC-225 series, NDC-255 series en: CPP3;
- Bosch Economy HD Box Cameras, NBC-265 series, NTC-265-PI en: CPP3;
- Bosch Economy HD Dome Cameras, NDC-265 series, NDN-265-PIO en: CPP3;
- Bosch Extreme series EX30 IR, NEI-30 IR Imager en: CPP3;
- Bosch FLEXIDOME 2X, NDN-498-P en: CPP3;
- Bosch FLEXIDOME HD 1080p en: CPP4;
- Bosch FLEXIDOME HD 1080p HDR en: CPP4;
- Bosch FLEXIDOME HD 720p en: CPP4;
- Bosch FLEXIDOME IP 3000i en: CPP7.3;
- Bosch FLEXIDOME IP 4000i en: CPP7.3;
- Bosch FLEXIDOME IP 5000i en: CPP7.3;
- Bosch FLEXIDOME IP indoor 4000 HD en: CPP4;
- Bosch FLEXIDOME IP indoor 4000 IR en: CPP4;
- Bosch FLEXIDOME IP indoor 5000 HD en: CPP4;
- Bosch FLEXIDOME IP indoor 5000 MP en: CPP4;
- Bosch FLEXIDOME IP micro 2000 HD en: CPP4;
- Bosch FLEXIDOME IP micro 2000 IP en: CPP4;
- Bosch FLEXIDOME IP micro 5000 HD en: CPP4;
- Bosch FLEXIDOME IP micro 5000 MP en: CPP4;
- Bosch FLEXIDOME IP outdoor 4000 HD en: CPP4;
- Bosch FLEXIDOME IP outdoor 4000 IR en: CPP4;
- Bosch FLEXIDOME IP outdoor 5000 HD en: CPP4;
- Bosch FLEXIDOME IP outdoor 5000 MP en: CPP4;
- Bosch FLEXIDOME IP panoramic 5000 en: CPP4;
- Bosch FLEXIDOME IP panoramic 6000 12MP 180 en: CPP6;
- Bosch FLEXIDOME IP panoramic 6000 12MP 180 IVA en: CPP6;
- Bosch FLEXIDOME IP panoramic 6000 12MP 360 en: CPP6;
- Bosch FLEXIDOME IP panoramic 6000 12MP 360 IVA en: CPP6;
- Bosch FLEXIDOME IP panoramic 7000 12MP 180 en: CPP6;
- Bosch FLEXIDOME IP panoramic 7000 12MP 180 IVA en: CPP6;
- Bosch FLEXIDOME IP panoramic 7000 12MP 360 en: CPP6;
- Bosch FLEXIDOME IP panoramic 7000 12MP 360 IVA en: CPP6;
- Bosch FLEXIDOME IP starlight 5000i (IR) en: CPP7.3;
- Bosch FLEXIDOME IP starlight 6000 en: CPP7;
- Bosch FLEXIDOME IP starlight 7000 en: CPP7;
- Bosch FLEXIDOME IP starlight 8000i en: CPP7.3;
- Bosch FLEXIDOME XF 720p , NDN-921-P en: CPP3;
- Bosch FLEXIDOME XF, NDC-455-P en: CPP3;
- Bosch FLEXIDOME corner 9000 MP en: CPP4;
- Bosch Far Infra-Red camera, VOT-320 en: CPP3;
- Bosch IP bullet 4000 HD en: CPP4;
- Bosch IP bullet 5000 HD en: CPP4;
- Bosch IP micro 2000 en: CPP4;
- Bosch IP micro 2000 HD en: CPP4;
- Bosch MIC IP PSU en: CPP3;
- Bosch MIC IP dynamic 7000 en: CPP4;
- Bosch MIC IP fusion 9000i en: CPP7.3;
- Bosch MIC IP starlight 7000 en: CPP4;
- Bosch MIC IP starlight 7000i en: CPP7.3;
- Bosch MIC IP starlight 7100i en: CPP7.3;
- Bosch MIC IP ultra 7100i en: CPP7.3;
- Bosch REG 1.5 IP y REG L2 en: CPP3;
- Bosch TINYON IP 2000 family en: CPP4;
- Bosch VG4 AUTODOME IP series en: CPP3;
- Bosch VG5 AUTODOME IP series en: CPP3;
- Bosch VIDEOJET connect 7000, VJC-7000 en: CPP-ENC;
- Bosch VIDEOJET decoder 3000, VJD-3000 en: CPP-ENC;
- Bosch VIDEOJET multi 4000 en: CPP5;
- Bosch VIP X1 XF Single-Channel H.264 Encoder en: CPP3;

- Bosch VIP-X1600-XFM4 en: CPP-ENC;
- Bosch VIP-X16XF-E en: CPP5;
- Bosch VJT-X20/X40XF-E en: CPP-ENC;
- Bosch VJT-XTCXF en: CPP-ENC;
- Bosch Vyal-proof FLEXIDOME HD 1080p en: CPP4;
- Bosch Vyal-proof FLEXIDOME HD 1080p HDR en: CPP4;
- Bosch Vyal-proof FLEXIDOME HD 720p en: CPP4;
- Bosch Video Conference Dome IVA en: CPP3;
- Bosch WLAN cameras NBC-255-W y NBC-265-W en: CPP3.

Descripción:

La vulnerabilidad, que fue descubierta por los investigadores de seguridad Victor Lomne y Thomas Roche, y fue revelada por NXP a Bosch, tiene severidad media y se basa en un ataque de canal lateral (*side channel*) para extraer la clave privada ECDSA (*Elliptic Curve Digital Signature Algorithm*).

Solución:

El chip vulnerable no se puede actualizar, no hay ninguna solución disponible, por lo que se deben considerar las medidas de mitigación enumeradas a continuación:

- reemplazar claves ECDSA por claves RSA,
- las claves correspondientes a un dispositivo perdido deben ser invalidadas en la CA correspondiente y la información de revocación del certificado,
- al deshacerse de la cámara debe realizarse un borrado de la misma antes de sacarla de servicio,
- actualizar los modelos de cámara a CPP13 y CPP14 que ya no utilizan el chip vulnerable.

Detalle:

Se ha descubierto una vulnerabilidad de canal lateral de ondas electromagnéticas en los microcontroladores de seguridad NXP SmartMX/P5x y en los microcontroladores de autenticación segura A7x, con CryptoLib hasta la versión 2.9. La vulnerabilidad podría permitir a un atacante extraer una clave privada ECDSA tras acceder físicamente al chip. Se ha asignado el identificador CVE-2021-3011 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Infraestructuras críticas, IoT, Vulnerabilidad

---

Escritura fuera de límites en múltiples productos de Dräger

Fecha de publicación: 04/03/2021

Importancia: Alta

Recursos afectados:

- CC-Vision Basic, versión 7.5.2 y anteriores;
- CC-Vision E-Cal, versión 7.2.4.8 y anteriores.

Descripción:

El investigador Mario Ceballos ha reportado a DrÃ¤ger una vulnerabilidad de severidad alta que podría permitir a un atacante ejecutar código malicioso o bloquear el sistema.

Solución:

Actualizar:

- CC-Vision Basic a la versión 7.5.3 u otra posterior;
- CC-Vision E-Cal a la versión 7.2.5.0 u otra posterior.

Detalle:

Debido a una vulnerabilidad de escritura fuera de límites, que podría provocar un desbordamiento de búfer, un atacante podría ejecutar código malicioso o bloquear el sistema al cargar o abrir archivos *.gdt*.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en productos 1734-AENTR de Rockwell Automation

Fecha de publicación: 05/03/2021

Importancia: Alta

Recursos afectados:

- 1734-AENTR Series B, versiones de la 4.001 a la 4.005, y de la 5.011 a la 5.017;
- 1734-AENTR Series C, versiones 6.011 y 6.012.

Descripción:

El investigador Adam Eliot, de Loon Security Team, ha reportado a Rockwell Automation 2 vulnerabilidades, una de severidad alta y otra de severidad media, que podrían permitir a un atacante remoto modificar datos de forma no autorizada en los dispositivos.

Solución:

Actualizar el *firmware* de:

- 1734-AENTR Series B a la versión 5.018;
- 1734-AENTR Series C a la versión 6.013.

Para una información más detallada, consultar la web del fabricante.

Detalle:

- Una vulnerabilidad de control de acceso inapropiado para solicitudes HTTP POST podría permitir a un atacante remoto y no autenticado enviar una solicitud, especialmente diseñada, que posibilitase la modificación de los ajustes de configuración del equipo. Se ha asignado el identificador CVE-2020-14504 para esta vulnerabilidad.
- Una vulnerabilidad de XSS (*Cross Site Scripting*) almacenado podría permitir a un atacante remoto y no autenticado almacenar un script malicioso dentro de la interfaz web, que al ejecutarse modificase valores de cadena en la página de inicio de la interfaz web. Se ha asignado el identificador CVE-2020-14502 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Avisos de seguridad de Siemens de marzo de 2021

Fecha de publicación: 09/03/2021

Importancia: Alta

Recursos afectados:

- Solid Edge SE2020, todas las versiones;
- Solid Edge SE2021, todas las versiones;
- SIMATIC S7-PLCSIM V5.4, todas las versiones;
- RUGGEDCOM RM1224, versión 6.3;
- SCALANCE M-800, versión 6.3;
- SCALANCE S615, versión 6.3;
- SCALANCE SC-600, todas las versiones 2.1 o posteriores, pero anteriores a 2.1.3;
- PLUSCONTROL 1st Gen, todas las versiones;
- SENTRON 3VA COM100/800, todas las versiones;
- SENTRON 3VA DSP800, todas las versiones afectadas únicamente por CVE-2020-17437;
- SENTRON PAC2200 (con CLP Approval), todas las versiones afectadas únicamente por CVE-2020-17437;
- SENTRON PAC2200 (con MID Approval), todas las versiones afectadas únicamente por CVE-2020-17437;
- SENTRON PAC2200 (sin MID Approval), todas las versiones afectadas únicamente por CVE-2020-17437;
- SENTRON PAC3200, todas las versiones anteriores a 2.4.7;
- SENTRON PAC3200T, todas las versiones afectadas únicamente por CVE-2020-17437;
- SIMATIC MV400 family, todas las versiones anteriores a 7.0.6;
- Solid Edge SE2020, todas las versiones anteriores a SE2020MP13;
- Solid Edge SE2021, todas las versiones anteriores a SE2021MP3;
- Solid Edge SE2021, versión SE2021MP3 únicamente afectada por CVE-2020-28385 y CVE-2021-27380;
- SINEMA Remote Connect Server, todas las versiones anteriores a 3.0;
- LOGO! 8 BM (incluidas variantes SIPLUS), todas las versiones;
- SCALANCE SC600 Family, todas las versiones anteriores a 2.0;
- SIMATIC NET CM 1542-1, todas las versiones;
- RUGGEDCOM RM1224, todas las versiones 4.3 y posteriores;
- SCALANCE M-800, todas las versiones 4.3 y posteriores;
- SCALANCE S615, todas las versiones 4.3 y posteriores;
- SCALANCE SC-600 Family, todas las versiones 2.0 o posteriores, pero anteriores a 2.1.3;
- SCALANCE X300WG, todas las versiones anteriores a 4.1;
- SCALANCE XM400, todas las versiones anteriores a 6.2;
- SCALANCE XR500, todas las versiones anteriores a 6.2;
- SCALANCE Xx200 Family, todas las versiones anteriores a 4.1.

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 25 avisos de seguridad, de los cuales 13 son actualizaciones.

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

- lectura fuera de límites,

- escritura fuera de límites,
- desreferencia a puntero no confiable,
- limitación incorrecta del nombre de la ruta a un directorio restringido (*path traversal*),
- advertencia insuficiente en la interfaz de usuario sobre operaciones peligrosas,
- bucle infinito,
- denegación de servicio,
- valores insuficientemente aleatorios en los ISN (Initial Sequence Numbers) de conexiones TCP,
- validación incorrecta de paquetes TCP RST entrantes,
- restricción inadecuada de XML Eternal Entity Reference (XXE),
- autorización incorrecta,
- gestión incorrecta de condiciones excepcionales,
- desbordamiento de búfer basado en pila (*stack*).

Para estas vulnerabilidades se han asignado los siguientes identificadores: CVE-2021-22643, CVE-2021-22645, CVE-2021-22647, CVE-2021-22649, CVE-2021-22651, CVE-2021-25673, CVE-2021-25674, CVE-2021-25675, CVE-2021-25676, CVE-2020-28388, CVE-2020-13987, CVE-2020-17437, CVE-2020-25241, CVE-2020-27632, CVE-2020-28385, CVE-2020-28387, CVE-2021-27380, CVE-2021-27381, CVE-2020-25239, CVE-2020-25240, CVE-2020-25236, CVE-2019-3823 y CVE-2021-25667.

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

---

Múltiples vulnerabilidades en productos Schneider Electric

Fecha de publicación: 10/03/2021

Importancia: Crítica

Recursos afectados:

- ION8650, todas las versiones anteriores a 4.40.1;
- ION8800, todas las versiones anteriores a 372;
- ION7650 (Hardware rev. 4 o anterior), todas las versiones anteriores a 376;
- ION7650 (Hardware rev. 5), todas las versiones anteriores a 416;
- ION7700/73xx, todas las versiones;
- ION83xx/84xx/85xx/8600, todas las versiones;
- ION7400, todas las versiones anteriores a 3.0.0;
- ION9000, todas las versiones anteriores a 3.0.0;
- PM8000, todas las versiones anteriores a 3.0.0;
- IGSS Definition (Def.exe) versión 15.0.0.21041 y anteriores.

Descripción:

Schneider Electric ha publicado múltiples vulnerabilidades que podrían provocar el reinicio del medidor, la ejecución remota de código, la lectura o escritura arbitraria de datos o la pérdida de datos.

Solución:

Actualizar:

- ION8650, V4.40.1;
- ION8800, V372;
- ION7650 (Hardware rev. 4 o anterior), V376;
- ION7650 (Hardware rev. 5), V416;
- ION7700/73xx, se encuentra sin soporte. El fabricante recomienda considerar su sustitución por alguno de los nuevos modelos (PowerLogic ION9000, PowerLogic PM8000, o PowerLogic ION7400);
- ION83xx/84xx/85xx/8600, se encuentra sin soporte. El fabricante recomienda considerar su sustitución por alguno de los nuevos modelos (PowerLogic ION8650);
- ION7400, V3.0.0;
- ION9000, V3.0.0;
- PM8000, V3.0.0;
- IGSS Definition (Def.exe), versión 15.0.0.21042.

Detalle:

- La restricción inapropiada de operaciones dentro de los límites del búfer de la memoria, podría hacer que el medidor se reinicie o permitir la ejecución remota de código. Se han asignado los identificadores CVE-2021-22713 y CVE-2021-22714 para estas vulnerabilidades.
- La restricción inapropiada de operaciones dentro de los límites del búfer de la memoria, podría permitir la pérdida de datos o a la ejecución remota de código cuando se importa un archivo CGF (Configuration Group File) malicioso a IGSS Definition. Se han asignado los identificadores CVE-2021-22709 y CVE-2021-22710.
- La restricción inapropiada de operaciones dentro de los límites del búfer de la memoria, podría permitir una condición de lectura o escritura arbitrarias cuando se importa un archivo CGF (Configuration Group File) malicioso a IGSS Definition. Se han asignado los identificadores CVE-2021-22711 y CVE-2021-22712.

Etiquetas: Actualización, Infraestructuras críticas, SCADA, Schneider Electric, Vulnerabilidad

---

Vulnerabilidad RCE en PLC WinProladder de Fatek

Automation

Fecha de publicación: 12/03/2021

Importancia: Alta

Recursos afectados:

Fatek Automation PLC WinProladder.

Descripción:

Francis Provencher {PRL}, en colaboración con ZDI de Trend Micro, ha publicado una vulnerabilidad 0day de tipo ejecución remota de código (RCE), con severidad alta, que afecta a PLC WinProladder de Fatek Automation.

Solución:

Esta vulnerabilidad se ha divulgado públicamente sin un parche, con el acuerdo del ICS-CERT, por lo que la única medida de mitigación recomendada es restringir la interacción con la aplicación.

Detalle:

Esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en las versiones afectadas de Fatek Automation PLC WinProladder. Se requiere la interacción del usuario para explotar esta vulnerabilidad, ya que la potencial víctima debe visitar una página maliciosa o abrir un archivo malicioso. El fallo específico se localiza en el análisis de los archivos PWD, debido a la falta de validación adecuada de los datos suministrados por el usuario, lo que podría generar un desbordamiento de enteros antes de escribir en la memoria.

Etiquetas: 0day, Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en productos de la familia UR de GE

Fecha de publicación: 17/03/2021

Importancia: Crítica

Recursos afectados:

GE informa de que las vulnerabilidades afectan a los siguientes productos de la familia UR (B30, B90, C30, C60, C70, C95, D30, D60, F35, F60, G30, G60, L30, L60, L90, M60, N60, T35, T60) de relés avanzados de protección y control:

- vulnerabilidades relacionadas con el soporte a SSH: versiones de *firmware* desde 7.4x hasta 8.0x (opción CyberSentry);
- vulnerabilidades del servidor web: todas las versiones de *firmware* anteriores a 8.1x;
- protección contra la carga involuntaria de *firmware*: todas las versiones de *firmware* anteriores a la 8.1x con opción de seguridad básica;
- disposiciones para desactivar el modo de fábrica: todas las versiones de *firmware* anteriores a la 8.1x con opción de seguridad básica;
- acceso al registro *Last-key pressed*: todas las versiones de *firmware* anteriores a la 8.1x con opción de seguridad básica;
- debilidad en el binario del gestor de arranque de UR: todas las versiones del gestor de arranque anteriores a 7.03/7.04.

Descripción:

SCADA-X, el programa CyTRICS del DOE (Departamento de Energía), Verve Industrial y VuMetri han reportado a GE 10 vulnerabilidades: 1 crítica, 5 altas y 4 medias.

Solución:

GE recomienda a los usuarios con versiones de *firmware* afectadas que actualicen sus dispositivos UR a la versión 8.10 o superior del *firmware* UR para resolver estas vulnerabilidades. El fabricante proporciona mitigaciones adicionales e información sobre estas vulnerabilidades en su aviso GES-2021-004.

Detalle:

- UR (*Universal Relay*) IED (*Intelligent Electronic Devices*), con variante de seguridad *Basic*, no permite la desactivación del *Factory Mode*, que se utiliza para el mantenimiento del IED por parte de un usuario *Factory*. Se ha asignado el identificador CVE-2021-27426 para esta vulnerabilidad crítica.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2016-2183, CVE-2013-2566, CVE-1999-1085, CVE-2021-27422, CVE-2021-27418, CVE-2021-27420, CVE-2021-27428, CVE-2021-27424 y CVE-2021-27430.

Etiquetas: Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

---

Denegación de servicio en Hitachi ABB Power

Grids AFS Series

Fecha de publicación: 17/03/2021

Importancia: Media

Recursos afectados:

Hitachi ABB Power Grids AFS Series, modelos AFS660/AFS665 versión 7.0.07 con las siguientes variantes:

- AFS660-SR,
- AFS665-SR.

Descripción:

Hitachi ABB Power Grids ha identificado una vulnerabilidad de severidad media que podría causar una denegación de servicio en la serie AFS en uno de los puertos de un anillo HSR.

Solución:

Hitachi ABB Power Grids ha publicado la versión 7.1.03 que soluciona esta vulnerabilidad modificando la forma en la que el conmutador procesa las tramas HSR.

Detalle:

La vulnerabilidad encontrada permite que una trama HSR manipulada pueda provocar una condición de denegación de servicio en uno de los puertos de un anillo HSR. Se ha asignado el identificador CVE-2020-9307 para esta vulnerabilidad

Etiquetas: Actualización, Infraestructuras críticas, SCADA, Vulnerabilidad

---

Vulnerabilidad XSS en WebAccess/SCADA de Advantech

Fecha de publicación: 17/03/2021

Importancia: Media

Recursos afectados:

WebAccess/SCADA, versión 9.0 y anteriores.

Descripción:

Chizuru Toyama, de TXOne IoT/ICS Security Recearch Labs perteneciente a Trend Micro, ha reportado al CISA una vulnerabilidad de severidad media que podría permitir a un atacante remoto secuestrar las *cookies* o *tokens* de sesión de un usuario o redirigirlo a una página web maliciosa.

Solución:

Actualizar a la versión 9.0.1 u otra posterior.

Detalle:

Una vulnerabilidad de XSS (*Cross Site Scripting*) podría permitir a un atacante, remoto y no autorizado, enviar código JavaScript malicioso a un usuario para así, secuestrar las *cookies* o *tokens* de su sesión, redirigirlo a una página web maliciosa o realizar acciones no deseadas en el navegador. Se ha asignado el identificador CVE-2021-27436 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, SCADA, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Hitachi ABB

Fecha de publicación: 19/03/2021

Importancia: Crítica

Recursos afectados:

- eSOMS, versiones 6.0 anteriores a la 6.0.4.2.2;
- eSOMS, versiones 6.1 anteriores a la 6.1.4;
- eSOMS, versiones anteriores a la 6.3;
- eSOMS, todas las versiones anteriores a la 6.3 que utilicen una versión de *software* Telerik.

Descripción:

Hitachi ABB Power Grids ha reportado al CISA múltiples vulnerabilidades, en sus productos eSOMS, que podrían permitir a un atacante leer y eliminar una imagen del servidor, realizar cargas de archivos arbitrarias, ejecutar código arbitrario o romper los mecanismos de protección criptográfica.

Solución:

- Actualizar a eSOMS, versiones 6.0.4.2.2, 6.1.4 o 6.3.
- Para más información puede ponerse en contacto con Hitachi ABB Power Grids contact-centers.

Detalle:

Las vulnerabilidades de severidad crítica son:

- La limitación inadecuada de una ruta de acceso a un directorio restringido (*path traversal*) podría permitir a un atacante remoto leer y eliminar una imagen con extensión .BMP, .EXIF, .GIF, .ICON, .JPEG, .PNG, .TIFF o .WMF en el servidor, a través de una solicitud especialmente diseñada. Se ha asignado el identificador CVE-2019-19790 para esta vulnerabilidad.
- Una vulnerabilidad de deserialización .NET en la función RadAsyncUpload podría ser explotada por un atacante que conozca las claves de cifrado. Se ha asignado el identificador CVE-2019-18935 para esta vulnerabilidad.
- Progress Telerik no restringe correctamente la entrada del usuario a RadAsyncUpload, lo que podría permitir a los atacantes remotos realizar cargas de archivos arbitrarias o ejecutar código arbitrario. Se ha asignado el identificador CVE-2017-11357 para esta vulnerabilidad.
- Telerik.Web.UI utiliza un cifrado débil de RadAsyncUpload, lo que podría permitir a los atacantes remotos realizar cargas de archivos arbitrarias o ejecutar código arbitrario. Se ha asignado el identificador CVE-2017-11317 para esta vulnerabilidad.
- La protección inadecuada de Telerik.Web.UI.DialogParametersEncryptionKey o MachineKey, podría permitir a los atacantes remotos romper los mecanismos de protección criptográfica, lo que llevaría a una fuga de MachineKey, cargas o descargas de archivos arbitrarios, XSS o al compromiso de ASP.NET ViewState. Se ha asignado el identificador CVE-2017-9248 para esta vulnerabilidad.

El resto de vulnerabilidades de severidad alta tienen asignados los identificadores CVE-2021-26845, CVE-2014-2217 y CVE-2014-4958.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Exposición de información en exacqVision Web Service de Johnson Controls

Fecha de publicación: 19/03/2021

Importancia: Media

Recursos afectados:

exacqVision Web Service, todas las versiones hasta la 20.12.2.0 incluida.

Descripción:

El investigador Milan Kyselica ha reportado a Johnson Controls una vulnerabilidad de severidad media que podría permitir a un atacante remoto acceder a información confidencial.

Solución:

Actualizar a la versión 21.03.3 u otra posterior.

Detalle:

Una vulnerabilidad en el producto afectado podría permitir a un atacante remoto y no autorizado acceder a información confidencial a nivel de sistema sobre el exacqVision Web Service o el sistema operativo. Se ha asignado el identificador CVE-2021-27656 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Escritura fuera de límites en múltiples productos de TRUMPF

Fecha de publicación: 23/03/2021

Importancia: Alta

Recursos afectados:

- TruControl, versiones desde la 2.14.0 hasta la 3.14.0, de los siguientes productos:
  - TruPulse,
  - TruDisk,
  - TruDiode,
  - TruFiber,
  - TruMicro2000,
  - TruMicro5000,
  - TruMicro6000,
  - TruMicro7000,
  - TruMicro8000,

- TruMicro9000,
- redpowerDirect.

Descripción:

Qualys Research Labs ha reportado al fabricante TRUMPF Laser GmbH una vulnerabilidad de escritura fuera de límites que afecta a múltiples dispositivos. El fabricante, a su vez, ha notificado esta vulnerabilidad al

Solución:

- Actualizar TruControl a la versión 3.16.0 o posteriores;
- contactar con su socio de servicio () para obtener instrucciones sobre cómo obtener el parche.

Detalle:

Una vulnerabilidad de desbordamiento de búfer basado en Heap, presente en *sudo*, podría permitir la escalada de privilegios a *root* a través de "sudoedit -s" y un argumento de línea de comandos que termina con un solo carácter de barra invertida. Un usuario autenticado podría explotar esta vulnerabilidad provocando pérdida de datos en el control del láser, parada de la producción o daños por cambio del control del láser. Se ha asignado el identificador CVE-2021-3156 para esta vulnerabilidad ya publicada en INCIBE-CERT.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en routers EDR-810 de Moxa

Fecha de publicación: 23/03/2021

Importancia: Alta

Recursos afectados:

EDR-810 Series, versiones de *firmware*:

- 5.7 y anteriores para la vulnerabilidad CVE-2014-2284;
- 5.1 y anteriores para el resto de vulnerabilidades.

Descripción:

BDU FSTEC ha reportado a Moxa 10 vulnerabilidades que podrían permitir a un atacante remoto originar una condición de denegación de servicio, realizar una escalada de privilegios, acceder a información confidencial y ejecutar código arbitrario.

Solución:

Actualizar el *firmware* a la versión correspondiente desde la página web de soporte del fabricante:

- 5.8 para la vulnerabilidad CVE-2014-2284;
- 5.3 para el resto de vulnerabilidades.

Detalle:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos:

- validación incorrecta de entrada;
- denegación de servicio;
- escalada de privilegios;
- exposición de información sensible;
- ejecución remota de código
- errores de cifrado;
- *man-in-the-middle*;
- control de acceso, permisos, privilegios;
- errores numéricos.

Para estas vulnerabilidades se han asignado los siguientes identificadores: CVE-2014-2284, CVE-2015-1788, CVE-2016-10012, CVE-2015-3195, CVE-2016-6515, CVE-2017-17562, CVE-2013-0169, CVE-2016-0703, CVE-2013-1813 y CVE-2010-2156.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en varios productos de GE

Fecha de publicación: 24/03/2021

Importancia: Crítica

Recursos afectados:

- MU320E, todas las versiones de *firmware* anteriores a 04A00.1;

- Reason DR60, todas las versiones de *firmware* anteriores a 02A04.1.

Descripción:

Tom Westenberg, investigador del Thales UK y el Thales OT Security Team, han reportado 6 vulnerabilidades a GE, 2 de severidad crítica, 3 altas y 1 baja, que podrían permitir a un atacante escalar privilegios, utilizar credenciales codificadas para tomar el control del dispositivo, tomar el control total del registrador digital de fallos (DFR) o ejecutar código de forma remota.

Solución:

Actualizar los productos afectados a las siguientes versiones de *firmware*:

- MU320E: 04A00.1 o posteriores;
- Reason DR60: 02A04.1 o posteriores.

Detalle:

- El *software* afectado contiene una contraseña en texto claro que podría permitir a un atacante tomar el control de la unidad de fusión utilizando esta credencial. Se ha asignado el identificador CVE-2021-27452 para esta vulnerabilidad crítica.
- El *software* afectado contiene una contraseña en texto claro que utiliza para su propia autenticación de entrada o para la comunicación de salida con componentes externos. Se ha asignado el identificador CVE-2021-27440 para esta vulnerabilidad crítica.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2021-27448, CVE-2021-27438, CVE-2021-27454 y CVE-2021-27450.

Etiquetas: Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

---

Múltiples vulnerabilidades en dispositivos cMT de Weintek

Fecha de publicación: 24/03/2021

Importancia: Crítica

Recursos afectados:

Los siguientes modelos y versiones del sistema operativo de cMT están afectados:

- cMT-SVR-1xx/2xx, versiones anteriores a 20210305;
- cMT-G01/G02, versiones anteriores a 20210209;
- cMT-G03/G04, versiones anteriores a 20210222;
- cMT3071/cMT3072/cMT3090/cMT3103/cMT3151, versiones anteriores a 20210218;
- cMT-HDM, versiones anteriores a 20210204;
- cMT-FHD, versiones anteriores a 20210208;
- cMT-CTRL01, versiones anteriores a 20210302.

Impacto:

Marcin Dudek, investigador del CERT.PL, ha reportado 3 vulnerabilidades al CISA, todas de severidad crítica, cuya explotación podría permitir a un atacante remoto, no autenticado, acceder a información sensible y ejecutar código arbitrario para obtener privilegios de *root*.

Solución:

Aplicar las actualizaciones descritas en el apartado *Solution* del aviso oficial del fabricante.

Detalle:

- La línea de productos Weintek cMT es vulnerable a la inyección de código, que podría permitir a un atacante remoto, no autenticado, ejecutar comandos con privilegios de *root* en el sistema operativo afectado. Se ha asignado el identificador CVE-2021-27446 para esta vulnerabilidad.
- La línea de productos Weintek cMT es vulnerable a varios controles de acceso inadecuados, que podrían permitir a un atacante no autentificado acceder y descargar remotamente información sensible y realizar acciones administrativas en nombre de un administrador legítimo. Se ha asignado el identificador CVE-2021-27444 para esta vulnerabilidad.
- La línea de productos Weintek cMT es vulnerable a una vulnerabilidad de XSS que podría permitir a un atacante remoto, no autentificado, inyectar código JavaScript malicioso. Se ha asignado el identificador CVE-2021-27442 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en TBox de Ovarro

Fecha de publicación: 24/03/2021

Importancia: Alta

Recursos afectados:

- TWinSoft, todas las versiones anteriores a la 12.4 y todas las versiones de firmware anteriores a la 1.46;
- TBoxLT2, todos los modelos;
- TBox MS-CPU32;
- TBox MS-CPU32-S2;
- TBox RM2, todos los modelos;
- TBox TG2, todos los modelos.

Descripción:

El investigador Uri Katz de Claroty ha reportado 5 vulnerabilidades de severidad alta que podrían permitir a un atacante remoto ejecutar código o causar una condición de denegación de servicio.

Solución:

Actualizar TWinSoft a la versión 12.4 y el firmware de TBox a la versión 1.46 a través de la sección de atención al cliente en la página web del fabricante.

Detalle:

- Una vulnerabilidad de control inapropiado en la generación de código podría permitir a un atacante ejecutar código malicioso aprovechando que el paquete 'ipk', que contiene la configuración de TWinSoft, puede ser cargado, extraído y ejecutado en TBox. Se ha asignado el identificador CVE-2021-22646 para esta vulnerabilidad.
- Una asignación incorrecta de permisos en las funciones para el acceso a archivos Modbus propias de TBox podría permitir a un atacante leer, modificar o eliminar archivos de configuración. Se ha asignado el identificador CVE-2021-22648 para esta vulnerabilidad.
- Un atacante podría causar una condición de denegación de servicio haciendo uso de tramas Modbus, especialmente diseñadas, aprovechando una vulnerabilidad de consumo no controlado de recursos. Se ha asignado el identificador CVE-2021-22642 para esta vulnerabilidad.
- Un atacante podría descifrar la contraseña de inicio de sesión mediante *sniffing* de las comunicaciones y ataques de fuerza bruta aprovechando una protección insuficiente de las credenciales. Se ha asignado el identificador CVE-2021-22640 para esta vulnerabilidad.
- TWinSoft utiliza clave de cifrado codificada en texto claro para el usuario 'TwinSoft'. Se ha asignado el identificador CVE-2021-22644 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Secuestro de DLL en productos Bosch

Fecha de publicación: 25/03/2021

Importancia: Alta

Recursos afectados:

- Bosch BVMS, versión anterior a 9.0.0;
- Bosch BVMS versiones 10.0 anteriores a la 10.0.2;
- Bosch BVMS versiones 10.1 anteriores a la 10.1.1;
- Bosch BVMS Viewer, versión anterior a 9.0.0;
- Bosch BVMS Viewer versiones 10.0 anteriores a la 10.0.2;
- Bosch BVMS Viewer versiones 10.1 anteriores a la 10.1.1;
- Bosch Configuration Manager, versión anterior o igual a 7.21.0078;
- Bosch DIVAR IP 7000 R2 con la configuración ?using vulnerable BVMS version';
- Bosch DIVAR IP all-in-one 5000 con la configuración ?using vulnerable BVMS version';
- Bosch DIVAR IP all-in-one 7000 con la configuración ?using vulnerable BVMS version';
- Bosch IP Helper, versión anterior o igual a 1.00.0008;
- Bosch Monitor Wall, versión anterior o igual a 10.00.0164;
- Bosch Video Client, versión anterior o igual a 1.7.6.079;
- Bosch Video Recording Manager, versión 3.71 y anteriores;
- Bosch Video Recording Manager, versiones 3.81 anteriores o iguales a la 3.81.0064;
- Bosch Video Recording Manager, versiones3.82 anteriores o iguales a la 3.82.0055;
- Bosch Video Streaming Gateway, versión anterior o igual a 6.45.10.

Descripción:

Varias aplicaciones de *software* de Bosch están afectadas por una vulnerabilidad que podría permitir a un atacante cargar código adicional en forma de DLL que es ejecutado durante el inicio de la aplicación vulnerable y en el contexto del usuario.

Solución:

- Se recomienda actualizar las aplicaciones de *software* de Bosch afectadas a una versión no vulnerable.
- Si no hay una actualización disponible, se recomienda a los usuarios seguir las mitigaciones y soluciones:
  - El *software* no instalado (por ejemplo, los propios instaladores y las aplicaciones portables) no debe ejecutarse desde directorios a los que puedan acceder otros usuarios, o directorios en los que puedan encontrarse DLL potencialmente maliciosas (por ejemplo, el directorio 'descargas' por defecto).
  - No hay una ruta segura conocida para este tipo de *software*, por lo que el impacto potencial depende del directorio desde el que se carga un instalador o una aplicación portable ("AppDir"):
    - Directorio 'descargas' por defecto: los binarios maliciosos pueden residir en la carpeta de descargas por defecto de un usuario debido a la interacción previa de éste (por ejemplo, haciendo clic en un enlace de descarga malicioso, visitando un sitio que consigue ejecutar un *drive-by-download*) y podrían ser cargados por un ejecutable. Como medida de mitigación, se recomienda a los usuarios mover los ejecutables del directorio de descargas a nuevos directorios no accesibles por otros usuarios y sólo iniciar los ejecutables desde allí. En general, se recomienda no ejecutar instaladores u otras aplicaciones directamente desde el directorio de descargas por defecto y no aceptar peticiones de descarga no solicitadas en un navegador.
    - Directorios a los que tienen acceso varios usuarios con pocos privilegios: si dicho directorio no ha sido

creado por el propio *software* (por ejemplo, un directorio temporal durante el tiempo de instalación), se trata esencialmente de un directorio de instalación no protegido y, por tanto, de una configuración del sistema vulnerable. Se recomienda encarecidamente no colocar los ejecutables en un directorio donde otros usuarios con pocos privilegios tengan permisos de escritura. Tenga en cuenta que los directorios creados por el usuario bajo C: (por ejemplo, C:/MiNuevaCarpeta) heredarían los permisos de escritura para todos los usuarios y, por lo tanto se desaconseja encarecidamente.

Detalle:

- La carga de una DLL a través de un elemento de ruta de búsqueda no controlada podría permitir a un atacante ejecutar código arbitrario en el sistema de la víctima. Para ello, es necesario que la víctima sea engañada para colocar una DLL maliciosa en el mismo directorio de aplicaciones que la aplicación IP Helper portátil. Se ha asignado el identificador CVE-2020-6771 para esta vulnerabilidad.
- La carga de una DLL, a través de un elemento de ruta de búsqueda no controlado, podría permitir a un atacante ejecutar código arbitrario en el sistema de la víctima. Esto afecta tanto al instalador como a la aplicación instalada. Se ha asignado el identificador CVE-2020-6785 para esta vulnerabilidad.
- La carga de una DLL a través de un elemento de ruta de búsqueda no controlada podría permitir a un atacante ejecutar código arbitrario en el sistema de la víctima. Para ello, es necesario que la víctima sea engañada para colocar una DLL maliciosa en el mismo directorio desde el que se inicia el instalador. Se han asignado los identificadores CVE-2020-6786, CVE-2020-6787, CVE-2020-6788 y CVE-2020-6789 para estas vulnerabilidades.
- La llamada a un ejecutable a través de un elemento de ruta de búsqueda no controlada podría permitir a un atacante ejecutar código arbitrario en el sistema de la víctima. Para ello, es necesario que la víctima sea engañada para colocar un .exe malicioso en el mismo directorio desde el que se inicia el instalador. Se ha asignado el identificador CVE-2020-6790 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad