Boletín de abril de 2021

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en Rexroth ActiveMover de Bosch

Fecha de publicación: 05/04/2021

Importancia: Alta

Recursos afectados:

- Rexroth ActiveMover, con la configuraciones:
  - ?using Profinet communication module (Rexroth no. 3842 559 445)';
  - ?using EtherNet/IP communication module (Rexroth no. 3842 559 444)'. Para las versiones anteriores a 3.0.26.x.

Descripción:

Múltiples vulnerabilidades, ambas de severidad alta, podrían permitir a un atacante provocar la pérdida inesperada de la comunicación cíclica, la interrupción de la comunicación acíclica o hacer que el dispositivo EtherNet/IP se bloquee sin posibilidad de recuperación.

Solución:

Bosch Rexroth recomienda utilizar el producto en una red aislada, sin acceso a Internet y aplicar las siguientes medidas de mitigación:

- Minimice la exposición a la red y asegúrese de que los productos no son accesibles a través de Internet.
- Aísle los productos afectados de la red corporativa mediante una segmentación de red/cortafuegos.
- Si es necesario el acceso remoto, utilice métodos seguros como las redes privadas virtuales (VPN).

Detalle:

- El protocolo de pila PROFINET IO Device V3, anterior a V3.14.0.7, no limita correctamente los recursos disponibles al gestionar los servicios de Read Implicit Request, en función del contenido de la solicitud, lo que podría permitir la pérdida inesperada de la comunicación cíclica o la interrupción de la comunicación acíclica. Se ha asignado el identificador CVE-2021-20986 para esta vulnerabilidad.
- Una vulnerabilidad de denegación de servicio y corrupción de memoria en Hilscher EtherNet/IP Core V2, anterior a V2.13.0.21, podría permitir a un atacante la inyección de código a través de la red o hacer que los dispositivos se bloqueen sin posibilidad de recuperación. Se ha asignado el identificador CVE-2021-20987 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en FactoryTalk AssetCentre de Rockwell Automation

Fecha de publicación: 05/04/2021

Importancia: Crítica

Recursos afectados:

FactoryTalk AssetCentre, versión 10.00 y anteriores.

Descripción:

Los investigadores Sharon Brizinov y Amir Preminger de Claroty han reportado a Rockwell Automation 9 vulnerabilidades de severidad crítica que podrían permitir a un atacante, remoto y no autenticado, ejecutar código arbitrario o realizar inyecciones SQL.

Solución:

Actualizar FactoryTalk AssetCentre a la versión 11 u otra superior.

Como medidas de mitigación adicionales, el fabricante recomienda:

- Utilizar las funciones de seguridad integradas siguiendo la guía QA46277.
- No ejecutar el software como administrador.
- Utilizar aplicaciones similares a Microsoft AppLocker.
- Seguir el principio de mínimos privilegios para los usuarios.

Detalle:

- Una vulnerabilidad de deserialización de datos no confiables en los servicios AosService.rem, ArchiveService.rem y LogService.rem podría permitir a un atacante, remoto y no autenticado, ejecutar comandos arbitrarios. Se han asignado los identificadores CVE-2021-27462, CVE-2021-27466 y CVE-2021-27470 para estas vulnerabilidades respectivamente.
- Una vulnerabilidad en la restricción del uso de funciones relacionadas con los servicios de comunicación remota de IIS podría permitir a un atacante, remoto y no autenticado, modificar datos confidenciales en FactoryTalk AssetCentre. Se ha asignado el identificador CVE-2021-27474 para esta vulnerabilidad.
- Una vulnerabilidad en la función SaveConfigFile del servicio RACompare podría permitir a un atacante, remoto y no autenticado, ejecutar comandos arbitrarios. Se ha asignado el identificador CVE-2021-27476 para esta vulnerabilidad.
- Vulnerabilidades en las funciones de los servicios SearchService, AosService.rem y ArchiveService.rem podrían permitir a un atacante, remoto y no autenticado, ejecutar sentencias SQL arbitrarias. Se han asignado los identificadores CVE-2021-27472, CVE-2021-27468 y CVE-2021-27464 para estas vulnerabilidades respectivamente.
- Una vulnerabilidad de deserialización de datos no confiables en los endpoints remotos .NET de componentes FactoryTalk AssetCentre podría permitir a un atacante, remoto y no autenticado, obtener acceso al servidor principal y máquinas asociadas. Se ha asignado el identificador CVE-2021-27460 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Denegación de servicio en múltiples productos de Hitachi ABB Power Grids

Fecha de publicación: 07/04/2021

Importancia: Alta

Recursos afectados:

- Relion 670 series, todas las revisiones de las versiones 1.1, 1.2.3, 2.0, 2.2.2 y 2.2.3;
- Relion 650 series, todas las revisiones de las versiones 1.1, 1.2, y 1.3;
- Relion 670/650 series, todas las revisiones de las versiones 2.1 y 2.2.0;
- Relion 670/650/SAM600-IO series versión 2.2.1, todas las revisiones;
- RTU500 CMU, versiones de *firmware* 7.x, 8.x, 9.x, 10.x, 11.x y 12.x;
- REB500, versiones 7.3, 7.4, 7.5 7.6, 8.2 y 8.3;
- TEGO1 unidad de servicio de FOX615 con ESW, versión R1D02 y anteriores;
- MSM, todas las versiones anteriores a 2.1.0;
- GMS600, versiones 1.3.0 y anteriores;
- PWC600, versiones 1.0 y 1.1.

Descripción:

Markus Mahrla, investigador de GAI NetConsult GmbH, y Lars Lengersdorf, investigador de Amprion GmbH, han reportado a Hitachi ABB Power Grids una vulnerabilidad, de severidad alta, que podría causar un reinicio del dispositivo afectado, generando una condición de denegación de servicio (DoS).

Solución:

Hitachi ABB Power Grids recomienda a los usuarios que apliquen las actualizaciones pertinentes lo antes posible, contactando con el fabricante para adquirir la versión de *firmware* concreta que solucione la vulnerabilidad.

En el apartado *4. MITIGATIONS* del enlace de referencia se pueden consultar las nuevas versiones desarrolladas por el fabricante para abordar la vulnerabilidad, tanto las ya publicadas como las planeadas.

Detalle:

Un atacante, con acceso a la red IEC 61850 y conocimiento de cómo reproducir el ataque, así como de las direcciones IP de los diferentes puntos de acceso IEC 61850, podría forzar el reinicio del dispositivo, lo que lo dejaría inoperativo durante aproximadamente 1 minuto. Esta vulnerabilidad solo afecta a los productos con interfaces IEC 61850. Se ha asignado el identificador CVE-2021-27196 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Subdesbordamiento de enteros en WinProladder de FATEK Automation

Fecha de publicación: 09/04/2021

Importancia: Alta

Recursos afectados:

WinProladder, versiones 3.30 y anteriores.

Descripción:

El investigador, Francis Provencher, en colaboración con ZDI de Trend Micro, ha reportado al CISA una vulnerabilidad de severidad alta que podría permitir a un atacante ejecutar código arbitrario.

Solución:

Por el momento, FATEK Automation no ha publicado una solución. Para más información, contactar con el fabricante.

Detalle:

Una vulnerabilidad de subdesbordamiento de enteros podría ocasionar la escritura fuera de límites y así, permitir a un atacante ejecutar código arbitrario. Se ha asignado el identificador CVE-2021-2748 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, Vulnerabilidad

Avisos de seguridad de Siemens de abril de 2021

Fecha de publicación: 13/04/2021

Importancia: Crítica

Recursos afectados:

- Tecnomatix RobotExpert, todas las versiones anteriores a 16.1;
- Nucleus NET, todas las versiones;
- Nucleus RTOS, versiones que incluyen los módulos DNS afectados;
- Nucleus Source Code, versiones que incluyen los módulos DNS afectados e IPv6 *stack*;
- Nucleus ReadyStart, todas las versiones;
- Nucleus 4, todas las versiones anteriores a 4.1.0;
- VSTAR, versiones que incluyen los módulos DNS afectados e IPv6 *stack*;
- SCALANCE X200-4P IRT, todas las versiones anteriores a 5.5.1;
- SCALANCE X201-3P IRT, todas las versiones anteriores a 5.5.1;
- SCALANCE X201-3P IRT PRO, todas las versiones anteriores a 5.5.1;
- SCALANCE X202-2 IRT, todas las versiones anteriores a 5.5.1;
- SCALANCE X202-2P IRT (incluye variantes SIPLUS NET), todas las versiones anteriores a 5.5.1;
- SCALANCE X202-2P IRT PRO, todas las versiones anteriores a 5.5.1;
- SCALANCE X204 IRT, todas las versiones anteriores a 5.5.1;
- SCALANCE X204 IRT PRO, todas las versiones anteriores a 5.5.1;
- SCALANCE X204-2 (incluye variantes SIPLUS NET), todas las versiones;
- SCALANCE X204-2FM, todas las versiones;
- SINEMA Remote Connect Server, todas las versiones anteriores a 3.0;
- TIM 4R-IE (incluye variantes SIPLUS NET), todas las versiones;
- TIM 4R-IE DNP3 (incluye variantes SIPLUS NET), todas las versiones;
- Solid Edge SE2020, todas las versiones anteriores a SE2020MP13;
- Solid Edge SE2020, versión SE2020MP13 (solo afectada por las vulnerabilidades CVE-2020-26997, CVE-2021-25678 y CVE-2021-27382);
- Solid Edge SE2021, todas las versiones anteriores a SE2021MP4;
- SIMOTICS CONNECT 400:
  - todas las versiones anteriores a 0.5.0.0;
  - todas las versiones 0.5.0.0 y superiores solo se ven afectadas por la vulnerabilidad CVE-2021-25677.
- Control Center Server (CCS):
  - todas las versiones anteriores a 1.5.0;
  - todas las versiones 1.5.0 y superiores solo se ven afectadas por la vulnerabilidad CVE-2019-18340.
- Siveillance Video Open Network Bridge, versiones:
  - 2020 R3,
  - 2020 R2,
  - 2020 R1,
  - 2019 R3,
  - 2019 R2,
  - 2019 R1,
  - 2018 R3,
  - 2018 R2.
- LOGO! Soft Comfort, todas las versiones.

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 31 avisos de seguridad, de los cuales 17 son actualizaciones.

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

- escritura fuera de límites,
- denegación de servicio,
- desbordamiento de búfer,
- envenenamiento de caché DNS,
- DNS *spoofing*,
- bucle infinito,
- fuga de memoria,
- omisión de autenticación,
- *man-in-the-middle*,
- autenticación insuficiente,
- validación incorrecta de los datos de entrada,
- divulgación de información sensible,
- condición de carrera,
- ejecución de código,
- lectura fuera de límites,
- uso de valores insuficientemente aleatorios,
- uso de credenciales en texto claro,
- limitación inadecuada de una ruta de acceso a un directorio restringido (*path traversal*),
- DLL *hijacking*,
- uso de algoritmo criptográfico no seguro,
- inyección SQL,
- XSS,
- gestión de *logging* insuficiente.

Para estas vulnerabilidades se han asignado los siguientes identificadores: CVE-2021-25670, CVE-2020-15795, CVE-2020-27009, CVE-2021-25668, CVE-2021-25669, CVE-2021-27393, CVE-2021-25663, CVE-2021-25664, CVE-2019-19956, CVE-2020-7595, CVE-2015-5219, CVE-2015-7855, CVE-2015-7871, CVE-2015-7973, CVE-2015-7974, CVE-2015-7977, CVE-2015-7979, CVE-2015-7705, CVE-2015-8138, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-4953, CVE-2016-4954, CVE-2020-28385, CVE-2020-26997, CVE-2021-25678, CVE-2021-27380, CVE-2021-27382, CVE-2020-27736, CVE-2020-27737, CVE-2020-27738, CVE-2021-25677, CVE-2020-27736, CVE-2020-27737, CVE-2020-27738, CVE-2021-25677, CVE-2021-27392, CVE-2020-25243, CVE-2020-25244, CVE-2019-13947, CVE-2019-18337, CVE-2019-18338, CVE-2019-18340, CVE-2019-18341, CVE-2019-18342, CVE-2019-19290, CVE-2019-19291, CVE-2019-19292, CVE-2019-19293, CVE-2019-19294 y CVE-2019-19295.

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

---

Múltiples vulnerabilidades en productos Schneider Electric

Fecha de publicación: 14/04/2021

Importancia: Alta

Recursos afectados:

- SHFK-MT-104 DIVG.424327.104-14;
- SHFK-MT-104 DIVG.424327.104-09;
- SHFK-MT-104 DIVG.424327.104-08;
- SHFK-MT-104 DIVG.424327.104-24;
- SHFK-MT-104 DIVG.424327.104-10;
- SHFK-MT-104 DIVG.424327.104-27;
- SHFK-MT-104 DIVG.424327.104-28;
- SHFK-MT-104 DIVG.424327.104-30;
- SHFK-MT-104 DIVG.424327.104-25;
- SHASU-MT-107 DIVG.424327.107-02;
- SHASU-MT-107 DIVG.424327.107-01;
- SHAIIS-MT-111 DIVG.424327.111-04;
- SHAIIS-MT-111 DIVG.424327.111-06;
- SHAIIS-MT-111 DIVG.424327.111-08;
- SHAIIS-MT-111 DIVG.424327.111-11;
- SHAIIS-MT-111 DIVG.424327.111-02;
- SHAIIS-MT-111 DIVG.424327.111-14;
- SHAIIS-MT-111 DIVG.424327.111-16;
- SHAIIS-MT-111 DIVG.424327.111-19;
- SHAIIS-MT-111 DIVG.424327.111-20;
- SHAIIS-MT-111 DIVG.424327.111-12;
- C-Bus Toolkit, versión 1.15.7 y anteriores.

Descripción:

Se han publicado varias vulnerabilidades, 5 de severidad alta y 2 medias, que podrían permitir a un atacante omitir la comprobación NTLM MIC o escalar privilegios.

Solución:

Aplicar:

- El parche de Microsoft para el CVE-2019-1040;
- el parche de Microsoft para el CVE-2019-0803;
- la actualización de C-Bus Toolkit a la versión 1.15.8.

Detalle:

- Una vulnerabilidad en el componente Win32k, de gestión incorrecta de los objetos en la memoria, podría permitir a un atacante la escalada de privilegios. Se ha asignado el identificador CVE-2019-0803 para esta vulnerabilidad.
- Una vulnerabilidad de gestión de privilegios inadecuada podría permitir la ejecución remota de código cuando un usuario sin privilegios modifica un archivo. Se ha asignado el identificador CVE-2021-22716 para esta vulnerabilidad.
- Una vulnerabilidad de limitación inadecuada de un nombre de ruta a un directorio restringido (*path traversal*) podría permitir la ejecución remota de código al procesar archivos de configuración. Se ha asignado el identificador CVE-2021-22717 para esta vulnerabilidad.
- Una vulnerabilidad de limitación inadecuada de un nombre de ruta a un directorio restringido (*path traversal*) podría permitir la ejecución remota de código al restaurar archivos de configuración. Se ha asignado el identificador CVE-2021-22718 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2021-22720 y CVE-2019-1040.

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

---

Liberación incorrecta de recursos en productos TOYOPUC de JTEKT Corporation

Fecha de publicación: 14/04/2021

Importancia: Alta

Recursos afectados:

- Todas las versiones de los siguientes productos de TOYOPUC-PC10. Series:
  - PC10G-CPU TCC-6353,
  - PC10GE TCC-6464,
  - PC10P TCC-6372,
  - PC10P-DP TCC-6726,
  - PC10P-DP-IO TCC-6752,
  - PC10B-P TCC-6373,
  - PC10B TCC-1021,
  - PC10B-E/C TCU-6521,
  - PC10E TCC-4737.
- Todas las versiones de los siguientes productos de TOYOPUC-Plus. Series:
  - Plus CPU TCC-6740,
  - Plus EX TCU-6741,
  - Plus EX2 TCU-6858,
  - Plus EFR TCU-6743,
  - Plus EFR2 TCU-6859,
  - Plus 2P-EFR TCU-6929,
  - Plus BUS-EX TCU-6900.
- Todas las versiones de los siguientes productos de TOYOPUC-PC3J/PC2J. Series:
  - FL/ET-T-V2H THU-6289,
  - 2PORT-EFR THU-6404.

Descripción:

Younes Dragoni, investigador de Nozomi Networks, ha reportado al CISA una vulnerabilidad, de severidad alta, que permitiría a un atacante interrumpir las comunicaciones Ethernet entre dispositivos.

Solución:

JTEKT Corporation recomienda a los usuarios seguir los pasos descritos en la sección *4. MITIGATIONS* del aviso del CISA.

Las solicitudes de información adicional pueden enviarse a JTEKT Corporation en .

Detalle:

Si la comunicación Ethernet del producto afectado es dejada en *open state* por un atacante, las comunicaciones Ethernet no pueden ser establecidas con otros dispositivos, dependiendo de la configuración de los parámetros de enlace. Se ha asignado el identificador CVE-2021-27458 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Asignación incorrecta de permisos para recursos críticos en WebAccess/SCADA de Advantech

Fecha de publicación: 14/04/2021

Importancia: Alta

Recursos afectados:

WebAccess/SCADA, versión 9.0.1 y anteriores.

Descripción:

El investigador, Chizuru Toyama, de TXOne IoT/ICS Security Research Labs de Trend Micro, ha reportado al CISA una vulnerabilidad de severidad alta que podría permitir a un atacante remoto realizar una escalada de privilegios.

Solución:

Actualizar a la versión 9.0.3 u otra posterior.

Detalle:

Una vulnerabilidad, de asignación incorrecta de permisos para recursos críticos en el portal WebAccess/SCADA, podría permitir a un atacante remoto, con pocos privilegios, actualizar la contraseña de administrador e iniciar sesión como tal para realizar una escalada de privilegios en el sistema. Se ha asignado el identificador CVE-2021-22669 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, IoT, SCADA, Vulnerabilidad

---

Múltiples vulnerabilidades en el portal web de OpenClinic GA

Fecha de publicación: 14/04/2021

Importancia: Crítica

Recursos afectados:

OpenClinic GA, versión 5.173.3.

Descripción:

Yuri Kramarz, investigador de Cisco Talos, ha reportado múltiples vulnerabilidades de inyección SQL, inyección de comandos y escalada de privilegios, que afectan al portal web de OpenClinic GA, siendo sus severidades 1 crítica, 1 alta y el resto medias.

Solución:

Actualizar OpenClinic GA a una versión posterior a 5.173.3.

Detalle:

- Solicitudes web, especialmente diseñadas, podrían provocar que se ejecutasen comandos en el servidor debido a una vulnerabilidad de inyección de comandos. Un atacante, no autenticado, podría aprovecharla para realizar una exfiltración de la base de datos, las credenciales de usuario y comprometer el sistema operativo subyacente. Se ha asignado el identificador CVE-2020-27227 para esta vulnerabilidad crítica.
- Sobrescribir el binario podría resultar en una escalada de privilegios debido a una vulnerabilidad de permisos por defecto incorrectos en la funcionalidad de instalación. Un atacante podría reemplazar un archivo para explotar esta vulnerabilidad. Se ha asignado el identificador CVE-2020-27228 para esta vulnerabilidad alta.

Para el resto de vulnerabilidades con severidad media se han asignado los identificadores: CVE-2020-27226, CVE-2020-27229, CVE-2020-27230, CVE-2020-27231, CVE-2020-27232, CVE-2020-27233, CVE-2020-27234, CVE-2020-27235, CVE-2020-27236, CVE-2020-27237, CVE-2020-27238, CVE-2020-27239, CVE-2020-27240, CVE-2020-27241, CVE-2020-27242, CVE-2020-27243, CVE-2020-27244, CVE-2020-27245 y CVE-2020-27246.

Etiquetas: Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

---

Múltiples vulnerabilidades en productos de Eaton

Fecha de publicación: 14/04/2021

Importancia: Alta

Recursos afectados:

- Eaton Intelligent power Manager (IPM), todas las versiones anteriores a la 1.69;
- Eaton Intelligent Power Manager Virtual Applicance (IPM VA), todas las versiones anteriores a la 1.69;
- Eaton Intelligent Power Protector (IPP), todas las versiones anteriores a la 1.68.

Descripción:

El investigador, Amir Preminger, de Claroty research, ha reportado 6 vulnerabilidades de severidad alta que podrían permitir a un atacante añadir usuarios a la base de datos, ejecutar comandos arbitrarios, eliminar información y cargar código malicioso.

Solución:

Actualizar Eaton IPM a la versión 1.69 y Eaton IPP a la versión 1.68.

Detalle:

- Una vulnerabilidad de inyección SQL en IPM podría permitir a un atacante autenticado añadir usuarios en la base de datos mediante el envío de un paquete especialmente diseñado. Se ha asignado el identificador CVE-2021-23276 para esta vulnerabilidad.
- Una vulnerabilidad de inyección de evaluación en IPM hace que el software no neutralice la sintaxis de código del usuario antes de llamar a la función *loadUserFile*, lo que podría permitir a un atacante no autenticado controlar la entrada a la función y ejecutar comandos arbitrarios. Se ha asignado el identificador CVE-2021-23277 para esta vulnerabilidad.
- Una vulnerabilidad de validación incorrecta de entrada en *server/maps_srv.js* y en *meta_driver_srv.js* podría permitir a un atacante, autenticado o no respectivamente, eliminar archivos del sistema donde está instalado el software IPM mediante el envío de paquetes especialmente diseñados. Se han asignado los identificadores CVE-2021-23278 y CVE-2021-23279 para estas vulnerabilidades.
- Una vulnerabilidad de carga de archivos arbitrarios en IPM podría permitir a un atacante autenticado cargar un archivo malicioso NodeJS o ejecutar comandos arbitrarios mediante el envío de un paquete especialmente diseñado. Se ha asignado el identificador CVE-2021-23280 para esta vulnerabilidad.
- Una vulnerabilidad de inyección de código en IPM podría permitir a un atacante no autenticado enviar un paquete especialmente diseñado para que IPM se conecte a un servidor SNMP y ejecutar código arbitrario. Se ha asignado el identificador CVE- 23281 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en OpENer EtherNet/IP de EIPStackGroup

Fecha de publicación: 16/04/2021

Importancia: Alta

Recursos afectados:

OpENer EtherNet/IP, *commits* y versiones anteriores al 10/02/2021.

Descripción:

Tal Keren y Sharon Brizinov, investigadores de Claroty, han reportado al CISA 4 vulnerabilidades, todas de severidad alta, que afectan a OpENer EtherNet/IP de EIPStackGroup y que podrían generar una condición de denegación de servicio (DoS) y exposición de información.

Solución:

El mantenedor de OpENer recomienda a los afectados aplicar los últimos *commits* disponibles.

Detalle:

- Un paquete, específicamente diseñado, enviado por un atacante a los dispositivos afectados podría causar una condición de denegación de servicio (DoS). Se han asignado los identificadores CVE-2021-27478, CVE-2021-27500 y CVE-2021-27498 para estas vulnerabilidades.
- Un paquete, específicamente diseñado, enviado por un atacante podría permitirle leer datos arbitrarios. Se ha asignado el identificador CVE-2021-27482 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Meinberg con LANTIME firmware

Fecha de publicación: 21/04/2021

Importancia: Alta

Recursos afectados:

Todos los productos con *firmware* LANTIME, anteriores a V7.02.003 y a V6.24.028.

Este *firmware* es utilizado en productos LANTIME serie M, serie IMS y SyncFire.

Descripción:

El fabricante, Meinberg ha informado de nuevas versiones de su *firmware* LANTIME que corrigen múltiples vulnerabilidades en componentes integrados de terceros y que afectan a OpenSSL, *sudo* y también a su interfaz web LTOS-Web-Interface. Estas vulnerabilidades podrían permitir a un atacante alterar el cifrado en las comunicaciones, realizar una escalada de privilegios, inyectar comandos o ejecutar una vulnerabilidad de tipo Cross-Site-Scripting.

Solución:

Se recomienda actualizar el *firmware* LANTIME a las versiones V7.02.003 y V6.24.028 disponibles en la web del fabricante.

Detalle:

Las vulnerabilidades solucionadas en el *firmware* LANTIME y que afectan a componentes integrados de terceros son las siguientes:

- OpenSSL: CVE-2021-3450, CVE-2021-23840, CVE-2021-23841 y CVE-2021-23840;
- *sudo*: CVE-2021-3156.

Meinberg también ha solucionado vulnerabilidades que afectan a su interfaz web y que permitirían a un atacante realizar ataques de inyección de comandos o de tipo Cross-Site-Scripting, estas vulnerabilidades se producen debido a la falta de validación de entrada de algunos campos en la interfaz web SyncMon. No se ha reservado ningún identificador CVE para estas vulnerabilidades.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, SCADA, SSL/TLS, Vulnerabilidad

---

Múltiples vulnerabilidades en productos de Delta Electronics

Fecha de publicación: 21/04/2021

Importancia: Crítica

Recursos afectados:

- COMMGR, versión 1.12 y anteriores;
- CNCSoft. versión 1.01.28 (con ScreenEditor versión 1.01.2) y anteriores;
- CNCSoft-B, versión 1.0.0.3 y anteriores.

Descripción:

Peter Cheng, investigador de CyberSpace Non-Attack Research Institute de Elex CyberSecurity, Inc., y Natnael Samson en colaboración con ZDI de Trend Micro, han reportado al CISA 4 vulnerabilidades, 1 de severidad crítica y 3 altas, cuya explotación podría permitir realizar ejecución remota de código (RCE), causar el fallo de la aplicación afectada o causar ejecución de código arbitrario.

Solución:

Actualizar a las siguientes versiones:

- COMMGR 1.13;
- CNCSoft ScreenEditor 1.01.30;
- CNCSoft-B 1.0.0.4 o posteriores.

Detalle:

- El producto afectado es vulnerable a un desbordamiento del búfer basado en la pila (*stack*), que podría permitir a un atacante ejecutar código remoto, lo que provocaría una condición de denegación de servicio (DoS) en el servidor de aplicaciones. Se ha asignado el identificador CVE-2021-27480 para esta vulnerabilidad crítica.
- El producto afectado es vulnerable a una lectura fuera de límites, lo que podría permitir a un atacante ejecutar código arbitrario. Se han asignado los identificadores CVE-2021-22668 y CVE-2021-22660 para estas vulnerabilidades altas.
- El producto afectado es vulnerable a una escritura fuera de límites, que podría permitir a un atacante ejecutar código arbitrario. Se ha asignado el identificador CVE-2021-22664 para esta vulnerabilidad alta.

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

---

Múltiples vulnerabilidades en conmutadores Stratix de Rockwell Automation

Fecha de publicación: 21/04/2021

Importancia: Alta

Recursos afectados:

- Stratix 5800: versiones 16.12.01 y anteriores;
- Stratix 8000: versiones 15.2 (7) E3 y anteriores;
- Stratix 5700: versiones 15.2 (7) E3 y anteriores;
- Stratix 5410: versiones 15.2 (7) E3 y anteriores;
- Stratix 5400: versiones 15.2 (7) E3 y anteriores.

Descripción:

Investigadores de Cisco informaron a Rockwell Automation de vulnerabilidades en sus conmutadores industriales, gestionados por Stratix, que podrían permitir a un atacante causar vulnerabilidades de denegación de servicio, escalada de privilegios no autorizada, secuestro de sesiones web, accesos no permitidos a rutas relativas o la inyección de comandos en los productos afectados.

Solución:

Rockwell Automation recomienda aplicar las siguientes soluciones:

- Stratix 5800: instalar la versión 17.04.01 o posterior, y si es posible desactivar el protocolo DECnet por completo o por interfaces.
- Stratix 8300: migrar el producto a una solución más actualizada.

Para todos los productos afectados se recomienda además seguir el principio de usuarios con privilegios mínimos y que el acceso a las cuentas de usuario solo se otorgue al personal estrictamente necesario. Puede consultar el aviso del fabricante para más información.

Rockwell Automation está trabajando en nuevos parches para solucionar estas vulnerabilidades, y como mitigación provisional recomienda:

- Utilizar en las redes donde se encuentren los sistemas de control industrial, segmentación en la infraestructura de red a través de *firewalls* para evitar el tráfico de fuentes no autorizadas o de la red empresarial.
- En los productos que lo permitan, utilizar la configuración de un interruptor a modo de *hardware* para bloquear cambios no autorizados, etc.
- Conectarse a los dispositivos desde equipos confiables, con medidas de seguridad básicas aplicadas, tales como la utilización de programas antivirus/*antimalware* o equipos actualizados o con acceso limitado a Internet.
- Minimizar la exposición de la red para todos los dispositivos y/o sistemas del sistema de control, confirmando que no son accesibles desde Internet.
- Cuando se requiera acceso remoto, utilizar métodos seguros, como redes privadas virtuales (VPN).

Detalle:

Cisco ha comunicado a Rockwell Automation varias vulnerabilidades en las que, a través de su CLI o uPNP y sus productos de software Cisco IOS y Cisco IOS XE, podrían verse afectados los conmutadores Stratix. Algunas de estas vulnerabilidades podrían permitir que un atacante autenticado recupere la contraseña del protocolo industrial común (CIP), y luego configure de forma remota el dispositivo afectado como un usuario, o causar una denegación de servicio a través del protocolo DECnet.

Adicionalmente, se ha identificado una vulnerabilidad en los conmutadores Stratix 5800, que podría permitir que un atacante físico no autenticado ejecute código persistente en el momento del arranque.

Se han asignado los siguientes identificadores para estas vulnerabilidades: CVE-2021-1392, CVE-2021-1403, CVE-2021-1352, CVE-2021-1442, CVE-2021-1452, CVE-2021-1443, CVE-2021-1220 y CVE-2021-1356.

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

---

Vulnerabilidad de XSS en productos Ellipse APM de Hitachi ABB Power Grids

Fecha de publicación: 21/04/2021

Importancia: Media

Recursos afectados:

- Ellipse APM, versión 5.3.0.1 y anteriores;
- Ellipse APM, versión 5.2.0.3 y anteriores;
- Ellipse APM, versión 5.1.0.6 y anteriores.

Descripción:

Hitachi ABB Power Grids ha reportado al CISA una vulnerabilidad de severidad media que podría permitir a un atacante autenticado o a una aplicación integrada inyectar datos maliciosos o ejecutar código arbitrario.

Solución:

Actualizar a las versiones 5.3.0.2, 5.2.0.4 y 5.1.0.7, respectivamente.

Detalle:

Una vulnerabilidad de XSS almacenado en el panel principal de los productos afectados podría permitir a un atacante autenticado o a una aplicación integrada inyectar datos maliciosos o ejecutar código arbitrario. Se ha asignado el identificador CVE-2021-27887 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Ejecución remota de código en Advantech WebAccess/HMI Designer

Fecha de publicación: 22/04/2021

Importancia: Alta

Recursos afectados:

WebAccess/HMI Designer.

Descripción:

kimiya, investigador de 9SG Security Team, ha reportado una vulnerabilidad 0day, con severidad alta, detectada en WebAccess/HMI Designer de Advantech.

Solución:

Esta vulnerabilidad se ha divulgando públicamente sin un parche, de acuerdo con el plazo de publicación de ZDI. La única estrategia de mitigación efectiva es restringir la interacción con la aplicación.

Detalle:

La vulnerabilidad se produce en el parseo de los archivos SNF, concretamente debido a la validación incorrecta de los datos suministrados por el usuario, lo que podría corromper la memoria, posibilitando que un atacante remoto ejecutase código arbitrario en las instalaciones afectadas de Advantech WebAccess/HMI Designer.

Etiquetas: 0day, Infraestructuras críticas, IoT, SCADA, Vulnerabilidad

---

Omisión de autenticación en Mitsubishi Electric GOT

Fecha de publicación: 26/04/2021

Importancia: Media

Recursos afectados:

Mitsubishi Electric informa que la vulnerabilidad afecta a la función VNC de los siguientes dispositivos:

- GOT2000 series:
  - modelo GT27, todas las versiones;
  - modelo GT25, todas las versiones;
  - modelo GT21, todas las versiones:
    - GT2107-WTBD, todas las versiones;
    - GT2107-WTSD, todas las versiones.
- GOT SIMPLE series:
  - modelo GS21:
    - GS2110-WTBD-N, todas las versiones;
    - GS2107-WTBD-N, todas las versiones.

Descripción:

Mitsubishi Electric ha reportado al CISA una vulnerabilidad, de severidad media, cuya explotación podría permitir a un atacante obtener acceso no autorizado.

Solución:

Mitsubishi Electric aún no ha publicado parche para la vulnerabilidad. Como medida de mitigación, indica a los usuarios que restrinjan el acceso al producto sólo desde redes y *hosts* de confianza.

Detalle:

Existe una vulnerabilidad, de omisión de autenticación de la contraseña, en la función VNC de la serie GOT2000 y la serie GOT SIMPLE debido a una autenticación incorrecta. Cuando la configuración del servidor VNC está activada, un atacante podría obtener acceso no autorizado enviando paquetes especialmente diseñados. Se ha asignado el identificador CVE-2021-20590 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, Virtualización, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Bosch

Fecha de publicación: 26/04/2021

Importancia: Crítica

Recursos afectados:

- Rexroth IoT Gateway;
- ctrlX CORE Runtime, versión XCR-V-0108.1 y anteriores.

Descripción:

Se han notificado múltiples vulnerabilidades en las librerías del sistema operativo y el kernel de Linux que podrían permitir a un atacante comprometer el sistema provocando un fallo o la ejecución de código malicioso.

Solución:

- Para el ctrlX CORE, las vulnerabilidades del kernel de Linux se abordan con la actualización XCR-V-0108.
- Para las vulnerabilidades de las bibliotecas del sistema operativo ctrlX CORE, está prevista una versión actualizada para el 05/2021. Póngase en contacto con su distribuidor para obtener instrucciones sobre cómo recuperar las

actualizaciones.

Se recomienda aplicar medidas de mitigación hasta que la actualización esté disponible. Puede encontrarlas en la 'Guía de seguridad de accionamientos y controles eléctricos'.

Detalle:

Las vulnerabilidades de severidad crítica se refieren a:

- En la utilidad de línea de comandos de Zstandard, versiones anteriores a la 1.4.1, los archivos de salida se creaban con permisos por defecto. Los permisos correctos de los archivos (que coincidían con los de entrada) sólo se establecían en el momento de la finalización. Por lo tanto, los archivos de salida podían ser leídos o escritos por personas no deseadas. Se ha asignado el identificador CVE-2021-24031 para esta vulnerabilidad.
- La utilidad de línea de comandos de Zstandard creaba archivos de salida con permisos por defecto y restringía esos permisos inmediatamente después. Por lo tanto, los atacantes podían leer o escribir estos archivos de salida. Se ha asignado el identificador CVE-2021-24032 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2020-27815, CVE-2020-27830, CVE-2020-28374, CVE-2020-28941, CVE-2020-29568, CVE-2020-29569, CVE-2020-29660, CVE-2020-29661, CVE-2021-24032, CVE-2021-27218, CVE-2021-27219, CVE-2021-27803, CVE-2020-27815, CVE-2020-27830, CVE-2020-28374, CVE-2020-28941, CVE-2020-29568, CVE-2020-29569, CVE-2020-29660, CVE-2020-29661, CVE-2021-20232, CVE-2021-24031, CVE-2021-24032, CVE-2021-27218, CVE-2021-27219 y CVE-2021-27803.

Etiquetas: Infraestructuras críticas, IoT, Linux, Vulnerabilidad

---

Múltiples vulnerabilidades en Cscape de Horner Automation

Fecha de publicación: 26/04/2021

Importancia: Alta

Recursos afectados:

Cscape, todas las versiones anteriores a la 9.90 SP4.

Descripción:

Sharon Brizinov, de Claroty, ha reportado dos vulnerabilidades a CISA que podrían permitir la ejecución de código en el contexto del proceso actual o la escalada local de privilegios.

Solución:

Actualizar a Cscape, versión 9.90 SP4.

Detalle:

- La validación inadecuada de los datos suministrados por el usuario al analizar los archivos del proyecto podría permitir a un atacante la corrupción de la memoria para ejecutar código en el contexto del proceso actual. Se ha asignado el identificador CVE-2021-22678 para esta vulnerabilidad.
- La configuración por defecto permite a todos los usuarios la instalación del producto, lo que permite permisos completos, incluyendo el acceso de lectura/escritura. Esto podría permitir a un atacante sin privilegios modificar los archivos binarios y de configuración para llevar a cabo una escalada local de privilegios. Se ha asignado el identificador CVE-2021-22682 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Yokogawa

Fecha de publicación: 26/04/2021

Importancia: Crítica

Recursos afectados:

- Exaopc R1.01.00 - R3.78.00;
- Exaquantum R1.10.00 - R3.20.00;
- ProSafe-RS R1.01.00 - R4.05.00. El siguiente paquete afecta a:
  - RS4E5100 Safety System Engineering and Maintenance Function,
  - RS4H2200 SOE OPC Interface Package.
- CENTUM VP (Including Entry Class) R4.01.00 - R6.07.10. El siguiente paquete afecta a VP6P6930 SEM OPC Interface Package.
- PRM R2.01.00 - R4.03.00;
- Field Wireless Device OPC Server R2.01.00, R2.01.01, R2.01.03, R2.01.10;
- STARDOM VDS R4.01 - R8.10;
- B/M9000 VP R7.01.01 - R8.03.00;
- CENTUM VP Controller FCS (Field Control Station), módulo de procesador FCS CP461, tipos de FCS:
  - AFV30S,
  - AFV30D,
  - AFV40S,

- AFV40D,
- A2FV50S,
- A2FV50D,
- A2FV70S,
- A2FV70D.

Descripción:

Yokogawa ha identificado varios productos vulnerables a RCE debido al uso de Microsoft Visual Basic 6.0 Runtime Extended Files y a ataques de canal lateral (*side-channel attacks*) ocasionado por las vulnerabilidades Meltdown/Spectre.

Solución:

Actualizar los productos afectados a las siguientes versiones o superiores:

- Exaopc R3.78.10;
- Exaquantum R3.20.02;
- ProSafe-RS R4.06.00;
- CENTUM VP R6.08.00 / R5.04.D3;
- PRM R4.04.00;
- Field Wireless Device OPC Server R2.01.11;
- STARDOM VDS R9.01;
- B/M9000 VP R8.03.53;
- CENTUM VP Controller FCS R6.08.00, o reemplazarlo por CP471.

Detalle:

- Se han encontrado productos de Yokogawa en los que se ha instalado la versión antigua de VB6 runtime con vulnerabilidades que podían permitir la ejecución remota de código si un usuario navegase por un sitio web con contenido especialmente diseñado.
- Varias versiones de CENTUM VP son vulnerables a Meltdown/Spectre, que afectan a implementaciones hardware de múltiples CPU.

Etiquetas: Actualización, Infraestructuras críticas, Microsoft, Vulnerabilidad

---

Múltiples vulnerabilidades en NPort IA5000A Series de Moxa

Fecha de publicación: 28/04/2021

Importancia: Alta

Recursos afectados:

- NPort IA5150A/IA5250A Series, versión de *firmware* 1.4 o anteriores;
- NPort IA5450A Series, versión de *firmware* 1.7 o anteriores.

Descripción:

Alexander Nochvay, invetigador de Kaspersky Lab ICS CERT, ha reportado a Moxa 4 vulnerabilidades que podrían permitir un control de acceso inadecuado, almacenamiento de credenciales sin protección o transmisión en claro de información sensible.

Solución:

- Para la vulnerabilidad CVE-2020-27149, actualizar:
  - NPort IA5150A/IA5250A Series: versión de *firmware* 1.5 o superiores;
  - NPort IA5450A Series: versión de *firmware* 2.0 o superiores.
- Para la vulnerabilidad CVE-2020-27149: los productos Moxa admiten una función de clave precompartida para codificar el archivo de configuración y mitigar este riesgo. Consulta la sección de *Export/Import* en el manual del usuario para más detalles.
- Para la vulnerabilidad CVE-2020-27184: los productos Moxa pueden desactivar el servicio Telnet para mitigar este riesgo. Consultar la sección *Console Settings* en el manual del usuario para más detalles. La versión de *firmware* 1.5 o superiores deshabilitará Telnet por defecto en NPort IA5150A/IA5250A Series. La versión de *firmware* 2.0 o superiores deshabilitará Telnet por defecto en NPort IA5450A Series.
- Para la vulnerabilidad CVE-2020-27185: los productos Moxa pueden desactivar el servicio Moxa para mitigar este riesgo. Consultar la sección *Console Settings* en el manual del usuario para más detalles.

Detalle:

- Un atacante podría explotar esta vulnerabilidad para escalar privilegios o para recibir peticiones que requieran un nivel de privilegio superior. Se ha asignado el identificador CVE-2020-27149 para esta vulnerabilidad.
- Un atacante podría extraer las credenciales de autenticación de un archivo de configuración enviado a través de un canal de comunicación inseguro, utilizando esos datos posteriormente para autenticarse a través del servicio Moxa y cambiar las configuraciones del dispositivo. Se ha asignado el identificador CVE-2020-27150 para esta vulnerabilidad.
- Un atacante podría leer todos los datos transferidos entre el cliente y el dispositivo si la comunicación se realiza a través de Telnet, incluyendo las credenciales de autenticación, los datos de configuración y la versión del dispositivo, y otros datos sensibles. Se ha asignado el identificador CVE-2020-27184 para esta vulnerabilidad.
- Un atacante podría leer todo el tráfico enviado cuando el servicio Moxa está habilitado, incluyendo datos de autenticación, configuraciones y versiones de dispositivos, y otros datos sensibles. Se ha asignado el identificador CVE-2020-27185 para esta vulnerabilidad.

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

---

Denegación de servicio en TwinCAT OPC UA Server e IPC Diagnostics UA Server de Beckhoff

Fecha de publicación: 28/04/2021

Importancia: Media

Recursos afectados:

- Servidor TwinCAT OPC UA, hasta la versión 2.3.0.12 incluida. Este producto está incluido en TF6100 OPC UA, y está afectado hasta la versión 3.3.18.
- Servidor UA de IPC Diagnostics, hasta la versión 3.1.0.1 incluida. Este producto se incluye preinstalado en los sistemas IPC de Beckhoff, aunque deshabilitado por defecto.

Descripción:

Beckhoff Automation ha informado que algunas versiones de TwinCAT OPC UA Server e IPC Diagnostics UA Server son vulnerables a ataques de denegación de servicio. Un atacante podría enviar varias solicitudes diseñadas específicamente al servidor OPC UA en ejecución y causar que deje de responder, provocando una denegación de servicio.

Solución:

- Para CX8091, Beckhoff recomienda actualizar a la versión de *firmware* "CX8091_CE600_LF_v356f_TC211R3_B2306_v2" o posterior.
- Para dispositivos que ejecutan Windows CE, Beckhoff recomienda que solicite una imagen reciente a través del soporte técnico.
- Para el resto de dispositivos que ejecutan otras versiones de Windows, Beckhoff recomienda que obtenga una versión reciente de los servidores OPC UA a través los canales de descarga oficiales.

Detalle:

Investigadores del Laboratorio de Seguridad de Control Industrial de QI-ANXIN Technology Group informaron al fabricante Beckhoff de una vulnerabilidad que permitiría a un atacante establecer una conexión TCP con uno de los servidores OPC UA afectados y enviarle una serie de paquetes de datos, específicamente diseñados, provocando un desbordamiento de pila por una incorrecta validación de entrada en el servidor OPC UA, haciendo que se detenga y requiera un reinicio por parte del administrador. Se ha asignado el identificador CVE-2020-12526 para esta vulnerabilidad.

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

Múltiples vulnerabilidades en productos Codesys

Fecha de publicación: 29/04/2021

Importancia: Alta

Recursos afectados:

CVE-2021-29242:

- Todas las variantes de los siguientes productos CODESYS V3, en todas las versiones anteriores a 3.5.17.0, que contengan el componente *CmpChannelServer*, *CmpChannelServerEmbedded*, *CmpRouter* o *CmpRouterEmbedded*, independientemente del tipo de CPU o del sistema operativo:
  - CODESYS Control RTE V3,
  - CODESYS Control RTE V3 (para Beckhoff CX),
  - CODESYS Control Win V3,
  - CODESYS Control V3 Runtime System Toolkit,
  - CODESYS V3 Embedded Target Visu Toolkit,
  - CODESYS V3 Remote Target Visu Toolkit,
  - CODESYS V3 Safety SIL2,
  - CODESYS Edge Gateway para Windows,
  - CODESYS Gateway V3,
  - CODESYS HMI V3,
  - CODESYS OPC Server V3,
  - CODESYS PLCHandler SDK,
  - CODESYS V3 Simulation Runtime (parte del CODESYS Development System).
- Los siguientes productos basados en CODESYS Control V3 Runtime System Toolkit están afectados en todas las versiones anteriores a 4.1.0.0:
  - CODESYS Control para BeagleBone SL,
  - CODESYS Control para emPC-A/iMX6 SL,
  - CODESYS Control para IOT2000 SL,
  - CODESYS Control para Linux SL,
  - CODESYS Control para Linux ARM SL,
  - CODESYS Control para PLCnext SL,
  - CODESYS Control para PFC100 SL,
  - CODESYS Control para PFC200 SL,
  - CODESYS Control para Raspberry Pi SL,
  - CODESYS Control para WAGO Touch Panels 600 SL,
  - CODESYS Edge Gateway para Linux.

CVE-2021-29240 y CVE-2021-29239: todas las versiones de CODESYS Development System V3 anteriores a 3.5.17.0, tanto

las variantes de 32 bits como las de 64 bits.

CVE-2021-29241:

- Todas las variantes de los siguientes productos CODESYS V3 que contienen el componente CmpGateway, independientemente del tipo de CPU o del sistema operativo:
  - CODESYS Edge Gateway para Linux (todas las versiones afectadas anteriores a 4.1.0.0);
  - CODESYS Control V3 Runtime System Toolkit (todas las versiones afectadas anteriores a 3.5.17.0);
  - CODESYS Development System (todas las versiones afectadas anteriores a 3.5.17.0);
  - CODESYS Edge Gateway para Windows (todas las versiones afectadas anteriores a 3.5.17.0);
  - CODESYS Gateway V3 (todas las versiones afectadas anteriores a 3.5.17.0).
- *CmpGateway* fue eliminado de los siguientes productos con las versiones especificadas a continuación. Por lo tanto, las versiones más recientes de estos productos ya no están afectadas:
  - CODESYS Control para BeagleBone SL (todas las versiones afectadas anteriores a 4.0.1.0);
  - CODESYS Control para emPC-A/iMX6 SL (todas las versiones afectadas anteriores a 4.0.1.0);
  - CODESYS Control para IOT2000 SL (todas las versiones afectadas anteriores a 4.0.1.0);
  - CODESYS Control para Linux SL (todas las versiones afectadas anteriores a 4.0.1.0);
  - CODESYS Control para PFC100 SL (todas las versiones afectadas anteriores a 3.5.16.0);
  - CODESYS Control para PFC200 SL (todas las versiones afectadas anteriores a 3.5.16.0);
  - CODESYS Control para Raspberry Pi SL (todas las versiones afectadas anteriores a 4.0.1.0).

CVE-2021-29238: versiones de CODESYS Automation Server, anteriores a 1.16.0, están afectadas. CODESYS GmbH ya ha actualizado todas las instancias a esta versión de corrección.

Descripción:

Diversos investigadores han reportado a Codesys 5 vulnerabilidades, todas de severidad alta, cuya explotación podría permitir a un atacante modificar paquetes de comunicación de bajo nivel, instalar paquetes maliciosos, editar o ejecutar archivos maliciosos, causar una condición de DoS o realizar una escalada de privilegios.

Solución:

CVE-2021-29242:

- Actualizar CODESYS GmbH a la versión 3.5.17.0 para solucionar la vulnerabilidad en los siguientes productos:
  - CODESYS Control RTE V3,
  - CODESYS Control RTE V3 (para Beckhoff CX),
  - CODESYS Control Win V3,
  - CODESYS Control V3 Runtime System Toolkit,
  - CODESYS V3 Embedded Target Visu Toolkit,
  - CODESYS V3 Remote Target Visu Toolkit,
  - CODESYS V3 Safety SIL2,
  - CODESYS Edge Gateway para Windows,
  - CODESYS Gateway V3,
  - CODESYS HMI V3,
  - CODESYS OPC Server V3,
  - CODESYS PLCHandler SDK,
  - CODESYS V3 Simulation Runtime (parte del CODESYS Development System).
- La vulnerabilidad se solucionará con la versión 4.1.0.0 (cuya publicación está planeada para mayo de 2021), que se basa en CODESYS Control V3 Runtime System Toolkit V3.5.17.0:
  - CODESYS Control para BeagleBone SL,
  - CODESYS Control para emPC-A/iMX6 SL,
  - CODESYS Control para IOT2000 SL,
  - CODESYS Control para Linux SL,
  - CODESYS Control para Linux ARM SL,
  - CODESYS Control para PLCnext SL,
  - CODESYS Control para PFC100 SL,
  - CODESYS Control para PFC200 SL,
  - CODESYS Control para Raspberry Pi SL,
  - CODESYS Control para WAGO Touch Panels 600 SL,
  - CODESYS Edge Gateway para Linux.

CVE-2021-29240 y CVE-2021-29239: CODESYS GmbH ha lanzado la versión 3.5.17.0 para resolver estas vulnerabilidades.

CVE-2021-29241:

- CODESYS GmbH ha lanzado la versión 3.5.17.0 para solucionar la vulnerabilidad en los siguientes productos:
  - CODESYS Control V3 Runtime System Toolkit,
  - CODESYS Gateway V3,
  - CODESYS Development System,
  - CODESYS Edge Gateway para Windows.
- Para CODESYS Edge Gateway, la vulnerabilidad se solucionará con la versión 4.1.0.0 (cuya publicación está planeada para mayo de 2021), que se basa en CODESYS Control V3 Runtime System Toolkit V3.5.17.0.

CVE-2021-29238: CODESYS GmbH ya ha actualizado todas las instancias de CODESYS Automation Server a la versión 1.16.0.

Detalle:

- Un atacante remoto podría enviar paquetes de comunicación, especialmente diseñados, para cambiar el esquema de direccionamiento de los routers y así como poder desviar, añadir, eliminar o cambiar paquetes de comunicación de bajo nivel entre los clientes y el sistema de ejecución de CODESYS Control. Se ha asignado el identificador CVE-2021-29242 para esta vulnerabilidad.
- El gestor de paquetes de CODESYS Development System no comprueba la validez de los paquetes antes de su instalación y podría utilizarse para instalar paquetes CODESYS con contenido malicioso local. Se ha asignado el identificador CVE-2021-29240 para esta vulnerabilidad.
- CODESYS Development System muestra o ejecuta documentos o archivos maliciosos insertados en librerías sin comprobar previamente su validez por parte de un atacante local. Se ha asignado el identificador CVE-2021-29239 para esta vulnerabilidad.
- Solicitudes de comunicación, especialmente diseñadas, podrían causar una desreferencia de puntero nulo (*null pointer*

dereference) en múltiples productos CODESYS, que podría dar lugar a una condición de denegación de servicio (DoS) llevada a cabo por un atacante remoto. Se ha asignado el identificador CVE-2021-29241 para esta vulnerabilidad.
- Un atacante remoto que manipulase los archivos de una CODESYS Web Visualization desplegada en un controlador, podría conducir a una escalada de privilegios cuando Web Visualization se abre con CODESYS Automation Server. Se ha asignado el identificador CVE-2021-29238 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Lectura arbitraria de archivos en Access Controller de Cassia Networks

Fecha de publicación: 30/04/2021

Importancia: Media

Recursos afectados:

Access Controller, todas las versiones anteriores a 2.0.1.

Descripción:

Amir Preminger y Sharon Brizinov, investigadores de Claroty, han reportado al CISA una vulnerabilidad, de severidad media, de limitación inadecuada a directorio restringido que afecta al producto Access Controller de Cassia Networks.

Solución:

Cassia Networks ha publicado un parche (es necesario iniciar sesión) que corrige la vulnerabilidad reportada.

Detalle:

Un atacante podría utilizar la ruta *minify* con una ruta relativa para ver cualquier archivo en el servidor de Access Controller. Se ha asignado el identificador CVE-2021-22685 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Texas Instruments SimpleLink

Fecha de publicación: 30/04/2021

Importancia: Crítica

Recursos afectados:

- SimpleLink MSP432E4 SDK, versión v4.20.00.12 y anteriores;
- SimpleLink CC32XX SDK, versión v4.30.00.06 y anteriores;
- SimpleLink CC13X0 SDK, versiones anteriores a la v4.10.03;
- SimpleLink CC13X2 SDK, versiones anteriores a la v4.40.00;
- SimpleLink CC26XX SDK, versiones anteriores a la v4.40.00;
- CC3200 SDK, versión v1.5.0 y anteriores;
- CC3100 SDK, versión v1.3.0 y anteriores.

Descripción:

David Atch y Omri Ben Bassat, de Microsoft, han reportado estas vulnerabilidades al CISA, que podrían permitir a un atacante la denegación del servicio o ejecución remota de código,

Solución:

Actualizar a las últimas versiones de software.

Detalle:

- Un desbordamiento de enteros en las API de la MCU del host, al intentar conectarse a una red wifi, podría permitir a un atacante la denegación de servicio o la ejecución de código. Se ha asignado el identificador CVE-2021-22677 para esta vulnerabilidad.
- Un desbordamiento de búfer basado en la pila, mientras se procesan las actualizaciones de *firmware over-the-air* desde el servidor CDN, podría permitir a un atacante la ejecución remota de código. Se ha asignado el identificador CVE-2021-22677 para esta vulnerabilidad.
- Un desbordamiento de enteros al analizar archivos de actualización de *firmware over-the-air*, podría permitir a un atacante la ejecución remota de código. Se ha asignado el identificador CVE-2021-22675 para esta vulnerabilidad.
- Un desbordamiento de enteros al procesar las cabeceras HTTP podría permitir a un atacante la ejecución remota de código. Se ha asignado el identificador CVE-2021-22679 para esta vulnerabilidad.
- Múltiples desbordamientos de enteros al procesar nombres de dominio largos, podría permitir a un atacante la ejecución remota de código. Se ha asignado el identificador CVE-2021-22671 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en sistemas operativos en tiempo real (RTOS)

Fecha de publicación: 30/04/2021

Importancia: Crítica

Recursos afectados:

- Amazon FreeRTOS, versión 10.4.1;
- Apache Nuttx OS, versión 9.1.0;
- ARM CMSIS-RTOS2, versiones anteriores a 2.1.3;
- ARM Mbed OS, versión 6.3.0;
- ARM mbed-uallaoc, versión 1.3.0;
- Software Cesanta Mongoose OS, versión v2.17.0;
- eCosCentric eCosPro RTOS, versiones 2.0.1 a 4.5.3;
- SDK de dispositivo de Google Cloud IoT, versión 1.0.2;
- Linux Zephyr RTOS, versiones anteriores a 2.4.0;
- Media Tek LinkIt SDK, versiones anteriores a 4.6.1;
- Micrium OS, versiones 5.10.1 y anteriores;
- Micrium uCOS II / uCOS III Versiones 1.39.0 y anteriores;
- NXP MCUXpresso SDK, versiones anteriores a 2.8.2;
- NXP MQX, versiones 5.1 y anteriores;
- Redhat newlib, versiones anteriores a 4.0.0;
- RIOT OS, versión 2020.01.1;
- Samsung Tizen RT RTOS, versiones anteriores a 3.0.GBB;
- TencentOS-tiny, versión 3.1.0;
- Texas Instruments CC32XX, versiones anteriores a 4.40.00.07;
- Texas Instruments SimpleLink MSP432E4XX;
- Texas Instruments SimpleLink-CC13XX, versiones anteriores a 4.40.00;
- Texas Instruments SimpleLink-CC26XX, versiones anteriores a 4.40.00;
- Texas Instruments SimpleLink-CC32XX, versiones anteriores a 4.10.03;
- Uclibc-NG, versiones anteriores a 1.0.36;
- Windriver VxWorks, anterior a 7.0.

Descripción:

Se han identificado múltiples vulnerabilidades en sistemas operativos en tiempo real (RTOS) de múltiples fabricantes, a través de un conjunto de vulnerabilidades relacionadas con el uso de funciones de asignación de memoria, como malloc, calloc, realloc, memalign, valloc, pvalloc, etc., y que se han dado a conocer en un informe denominado 'BadAlloc', Estas vulnerabilidades podrían permitir a un atacante realizar una ejecución remota de código o causar un bloqueo del sistema afectado.

Solución:

- Amazon FreeRTOS: descargar actualización;
- Apache Nuttx OS Versión 9.1.0: descargar actualización;
- ARM CMSIS-RTOS2: actualización en curso, prevista para junio;
- ARM Mbed OS: descargar actualización;
- ARM mbed-uallaoc: es un sistema obsoleto y no se realizara ninguna actualización;
- Cesanta Software mongooses: descargar actualización;
- eCosCentric eCosPro RTOS: actualización a las versiones 4.5.4 y posteriores;
- SDK de dispositivos de Google Cloud IoT: descargar actualización;
- Media Tek LinkIt SDK: MediaTek proporcionará la actualización a los usuarios. No hay solución para la versión gratuita, ya que no está diseñada para uso de producción;
- Micrium OS: actualización a versión 5.10.2 o posterior;
- Micrium uCOS-II / uCOS-III: actualización a versión 1.39.1: Actualización aún no publicada;
- NXP MCUXpresso SDK: actualización a versión 2.9.0 o posterior;
- NXP MQX: actualización a 5.1 o posterior;
- Redhat newlib: descargar actualización;
- RIOT OS: descargar actualización;
- Samsung Tizen RT RTOS: descargar actualización;
- TencentOS-tiny: descargar actualización;
- Texas Instruments CC32XX: actualización a v4.40.00.07;
- Texas Instruments SimpleLink CC13X0: actualización a v4.10.03; actualización aún no publicada;
- Texas Instruments SimpleLink CC13X2-CC26X2: actualización a v4.40.00; actualización aún no publicada;
- Texas Instruments SimpleLink CC2640R2: actualización a v4.40.00; actualización aún no publicada;
- Texas Instruments SimpleLink MSP432E4: confirmado. Actualmente no hay ninguna actualización planificada;
- uClibc-ng: descargar actualización;
- Windriver VxWorks: actualización en curso.

Adicionalmente, CISA recomienda a los usuarios afectados las siguientes medidas de mitigación:

- Minimice la exposición de la red para todos los dispositivos, en especial desde Internet.
- Ubique las redes del sistema de control y los dispositivos remotos detrás de firewalls, y separados de la red empresarial.
- Cuando se requiera acceso remoto, utilice métodos seguros, como redes privadas virtuales (VPN).

Detalle:

Los investigadores, David Atch, Omri Ben Bassat y Tamir Ariel, del equipo Sección 52 de Microsoft, integrado como equipo de investigación de seguridad Azure Defender para IoT, han descubierto un conjunto de vulnerabilidades críticas de asignación de memoria en dispositivos IoT y OT. Estas vulnerabilidades, denominadas 'BadAlloc', afectan a las funciones de asignación de memoria estándar que abarcan sistemas operativos en tiempo real (RTOS) de diferentes fabricantes, kits de desarrollo de

software integrados (SDK) e implementaciones de bibliotecas estándar C (libc).

Las vulnerabilidades encontradas se deben al uso de funciones de asignación de memoria vulnerables, como malloc, calloc, realloc, memalign, valloc, pvalloc, etc. La implementación de estas funciones en los productos afectados no ha incorporado las validaciones de entrada adecuadas. Sin estas validaciones de entrada, un atacante podría aprovechar la función de asignación de memoria para realizar un desbordamiento de la pila, lo que provocaría la ejecución de código malicioso en el dispositivo.

Se han asignado los siguientes identificadores para estas vulnerabilidades: CVE-2021-30636, CVE-2021-27431, CVE-2021-27433, CVE-2021-27435, CVE-2021-27427, CVE-2021-22684, CVE-2021-27439, CVE-2021-27425, CVE-2021-26461, CVE-2020-35198, CVE-2020-28895, CVE-2021-31571, CVE-2021-31572, CVE-2021-27417, CVE-2021-3420, CVE-2021-27411, CVE-2021-26706, CVE-2021-27421, CVE-2021-22680, CVE-2021-27419, CVE-2021-27429, CVE-2021-22636, CVE-2021-27504 y CVE-2021-27502.

Etiquetas: Actualización, Apache, Comunicaciones, Infraestructuras críticas, IoT, Linux, Vulnerabilidad

---

Escalada de privilegios en productos Johnson Controls

Fecha de publicación: 30/04/2021

Importancia: Alta

Recursos afectados:

- Serie Z y Serie A basadas en Linux,
- Serie Q,
- Serie G,
- Serie LC heredada,
- Serie ELP heredada,
- Grabadores de vídeo en red exacqVision (NVR),
- Estaciones de trabajo de la serie C basadas en Linux,
- Servidores de almacenamiento de la serie S.

Descripción:

Johnson Controls ha reportado esta vulnerabilidad al CISA que podría permitir a un atacante la escalada de privilegios.

Solución:

Johnson Controls recomienda a los usuarios que instalen las últimas actualizaciones de seguridad del sistema operativo Ubuntu Linux.

Detalle:

Unas vulnerabilidades de seguridad en las versiones del grabador de vídeo en red exacqVision, utilizadas en el sistema operativo Ubuntu Linux, afectan a la aplicación integrada Sudo, que controla el suministro de acceso de superusuario (administrador) al sistema operativo. Esto podría permitir a un atacante la escalada de privilegios no autorizada de superusuario al sistema operativo Ubuntu subyacente. Se ha asignado el identificador CVE-2021-3156 para esta vulnerabilidad.

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