Boletín de julio de 2020

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en Automation Worx Software Suite de Phoenix Contact

Fecha de publicación: 01/07/2020

Importancia: Alta

Recursos afectados:

Los componentes de Automation Worx Software Suite con versión 1.87 y anteriores:

- PC Worx,
- PC Worx Express.

Descripción:

Investigadores independientes trabajando a través de Trend Micro Zero Day Initiative han reportado varias vulnerabilidades en componentes de Worx Software Suite, que podrían permitir a un atacante comprometer la estación de trabajo donde se utilicen esos componentes a través de una ejecución remota de código.

Solución:

Esta vulnerabilidad se corregirá en la próxima versión de Automation Worx Software Suite.

Se recomienda no intercambiar archivos de proyectos para PC Worx de manera insegura o sin haber comprobado antes el cálculo de un *hash* de verificación de los ficheros para asegurar su integridad.

Detalle:

Las vulnerabilidades encontradas podrían permitir, mediante el uso de proyectos para PC Worx manipulados, realizar una ejecución remota de código debido a una insuficiente validación de entrada al procesar archivos *.mwe, provocando un desbordamiento de búfer basado en *stack* y lectura fuera de límites.

Un atacante necesitaría tener acceso a un proyecto original de PC Worx y manipular los datos dentro de la carpeta de proyectos, sustituyendo el manipulado por el original en la estación de trabajo.

Se han asignado los identificadores CVE-2020-12497 y CVE-2020-12498 para estas vulnerabilidades.

Etiquetas: Infraestructuras críticas, Privacidad, SCADA, Virtualización, Vulnerabilidad

Múltiples vulnerabilidades en varios productos de Mitsubishi Electric

Fecha de publicación: 01/07/2020

Importancia: Alta

Recursos afectados:

Las siguientes versiones de los productos de *software* de ingeniería de Factory Automation se ven afectadas:

- CPU Module Logging Configuration Tool, versiones 1.94Y y anteriores;
- CW Configurator, versiones 1.010L y anteriores;
- EM Software Development Kit (EM Configurator), versiones 1.010L y anteriores;
- GT Designer3?GOT2000), versiones 1.221F y anteriores;

- GX LogViewer, versiones 1.96A y anteriores;
- GX Works2, versiones 1.586L y anteriores;
- GX Works3, versiones 1.058L y anteriores;
- M_CommDTM-HART, versión 1.00A;
- M_CommDTM-IO-Link, versiones 1.02C y anteriores;
- MELFA-Works, versiones 4.3 y anteriores;
- MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool, versiones 1.004E y anteriores;
- MELSOFT FieldDeviceConfigurator, versiones 1.03D y anteriores;
- MELSOFT iQ AppPortal, versiones 1.11M y anteriores;
- MELSOFT Navigator, versiones 2.58L y anteriores;
- MI Configurator, versiones 1.003D y anteriores;
- Motion Control Setting, versiones 1.005F y anteriores;
- MR Configurator2, versiones 1.72A y anteriores;
- MT Works2, versiones 1.156N y anteriores;
- RT ToolBox2, versiones 3.72A y anteriores;
- RT ToolBox3, versiones 1.50C y anteriores.

Descripción:

Mitsubishi Electric PSIRT (*Product Security Incident Response Team*) reportó a CISA 2 vulnerabilidades, una de criticidad alta y otra media, de tipo restricción incorrecta de referencia a entida externa XML (XXE) y consumo de recursos incontrolado, que afectan a varios productos de Factory Automation.

Solución:

Mitsubishi Electric recomienda que los usuarios afectados descarguen la última versión de cada producto de *software* del centro de descargas de Mitsubishi Electric y lo actualicen.

Detalle:

- La vulnerabilidad podría permitir que un atacante malintencionado envíe un archivo al exterior en el equipo que ejecuta el producto afectado. Se ha asignado el identificador CVE-2020-5602 para esta vulnerabilidad.
- La vulnerabilidad podría permitir que un atacante malintencionado genere una condición de denegación de servicio (DoS) en el producto afectado. Se ha asignado el identificador CVE-2020-5603 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en Delta Industrial Automation DOPSoft de Delta Electronics

Fecha de publicación: 01/07/2020

Importancia: Alta

Recursos afectados:

DOPSoft, versiones 4.00.08.15 y anteriores.

Descripción:

La explotación exitosa de las 2 vulnerabilidades publicadas, de severidades alta y media, podría permitir a un atacante leer/modificar la información, ejecutar código arbitrario y/o bloquear la aplicación.

Solución:

Actualizar a la versión 4.00.08.17 o posteriores (previstas para julio de 2020).

Detalle:

- Múltiples vulnerabilidades de lectura fuera de límites podrían permitir a un atacante leer información y/o bloquear la aplicación mediante el procesamiento de archivos de proyecto especialmente diseñados. Se ha asignado el identificador CVE-2020-10597 para esta vulnerabilidad.
- La apertura de un archivo de proyecto especialmente diseñado puede desbordar la pila (heap), lo que podría permitir a un atacante la ejecución remota de código, la divulgación/modificación de información o hacer que la aplicación se bloquee. Se ha asignado el identificador CVE-2020-14482 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en Linear eMerge 50P/5000P de Nortek

Fecha de publicación: 03/07/2020

Importancia: Crítica

Recursos afectados:

Linear eMerge 50P/5000P, versiones 4.6.07 (revisión 79330) y anteriores.

Descripción:

Gjoko, de Applied Risk, ha reportado a CISA 5 vulnerabilidades, 3 de severidad crítica, una alta y una media, que podrían permitir a un atacante remoto ganar el control total del sistema.

Solución:

Actualizar a la versión v32-09a.

Detalle:

- El *software* utiliza entradas externas para construir una ruta que debería estar dentro de un directorio restringido, pero no neutraliza adecuadamente las secuencias como "../" que podrían resolverse a una ubicación que está fuera de ese directorio. Esto podría permitir a un atacante atravesar el sistema de archivos para acceder a los archivos o directorios que están fuera del directorio restringido. Se ha asignado el identificador CVE-2019-7267 para esta vulnerabilidad.
- La neutralización inadecuada de los caracteres especiales en los datos de entrada podría permitir a un atacante ejecutar comandos arbitrarios en el sistema operativo. Se ha asignado el identificador CVE-2019-7269 para esta vulnerabilidad.
- La ausencia de validación de la extensión de los archivos al subirlos a través del script de subida de la actualización del firmware podría permitir a un atacante remoto, no autenticado, subir archivos con extensiones arbitrarias a un directorio dentro de la raíz web de la aplicación y ejecutarlos con privilegios del servidor web. Se ha asignado el identificador CVE-2019-7268 para esta vulnerabilidad.
- La aplicación afectada permite a los usuarios realizar ciertas acciones a través de solicitudes HTTP sin realizar ninguna comprobación de validez para verificar dichas solicitudes. Esto podría ser explotado para realizar ciertas acciones con privilegios administrativos si un usuario conectado visita un sitio web malicioso. Se ha asignado el identificador CVE-2019-7270 para esta vulnerabilidad.
- La validación insuficiente de los datos de entrada podría permitir a un atacante remoto enviar una solicitud HTTP, especialmente diseñada, para pasar por alto las comprobaciones de autenticación y obtener acceso no autorizado a la aplicación. Se ha asignado el identificador CVE-2019-7266 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad Cross-site Scripting en ABB System 800xA Information Manager

Fecha de publicación: 03/07/2020

Importancia: Alta

Recursos afectados:

System 800xA Information Manager, versiones:

- anteriores a 5.1 Rev E/5.1 FP4 Rev E TC6;
- anteriores a 6.0.3.3 RU1;
- anteriores a 6.1 RU1.

Descripción:

El investigador William Knowles ha reportado una vulnerabilidad de tipo Cross-site Scripting en ABB System 800xA Information Manager que permitiría inyectar y ejecutar código arbitrario en el servidor.

Solución:

Esta vulnerabilidad se corrige en las siguientes versiones de ABB System 800xA Information Manager:

- 5.1 Rev E/5.1 FP4 E TC6: ABB recomienda a los usuarios en la rama 5.1 que instalen este TC, que se puede obtener a través de una petición al soporte técnico;
- 6.0.3.3 RU1: ABB recomienda a los usuarios de la rama 6.0.3 LTS que actualicen 6.0.3.3 e instalen RU1;
- 6.1 RU1: ABB recomienda a los usuarios de la rama 6.1 que actualicen a esta versión.

Los paquetes acumulativos de Information Manager para 6.0.3.3 y 6.1 se pueden descargar desde My ABB/My Control System.

Detalle:

La vulnerabilidad reportada en ABB System 800xA Information Manager podría permitir que un atacante ejecute código arbitrario de forma remota a través de un Cross-site Scripting. Para utilizar esta vulnerabilidad el atacante necesita engañar a un usuario con el componente de Information Manager vulnerable instalado en su equipo para que visite un sitio web manipulado. Se ha asignado el identificador CVE-2020-8477 para esta vulnerabilidad

Etiquetas: Actualización, Infraestructuras críticas, SCADA, Vulnerabilidad

---

Múltiples vulnerabilidades en OpenClinic GA

Fecha de publicación: 03/07/2020

Importancia: Crítica

Recursos afectados:

- OpenClinic GA, versión 5.09.02;
- OpenClinic GA, versión 5.89.05b.

Descripción:

Brian D. Hysell reportó 12 vulnerabilidades a CISA que afectan al sistema de gestión de información hospitalaria OpenClinic GA, repartidas en 3 de severidad crítica, 6 altas y 3 medias.

Solución:

OpenClinic GA es consciente de estas vulnerabilidades, pero no ha proporcionado ninguna confirmación de su resolución. Se recomienda actualizar OpenClinic GA a la última versión disponible para asegurarse de tener todas las correcciones actuales.

Detalle:

Las 3 vulnerabilidades con severidad crítica se describen a continuación:

- Un atacante podría omitir los controles de acceso del lado del cliente o usar una solicitud especialmente diseñada para iniciar una sesión con funcionalidad limitada, lo que podría permitir la ejecución de funciones de administrador, como consultas SQL. Se ha reservado el identificador CVE-2020-14485 para esta vulnerabilidad.
- El sistema contiene versiones de *software* de terceros que están al final de su ciclo de vida útil y contienen vulnerabilidades conocidas, que podrían permitir la ejecución remota de código. Se ha reservado el identificador CVE-2020-14495 para esta vulnerabilidad.
- El sistema posee una cuenta de usuario predeterminada oculta a la que se puede acceder si un administrador no ha desactivado expresamente esta cuenta, lo que podría permitir que un atacante inicie sesión y ejecute comandos arbitrarios (no afecta a la versión 5.89.05b). Se ha reservado el identificador CVE-2020-14487 para esta vulnerabilidad.

El resto de vulnerabilidades podrían ser aprovechadas por un atacante para realizar las siguientes acciones:

- ataques de fuerza bruta, debido a una restricción inadecuada ante un número excesivo de intentos de autenticación;
- acceso al sistema, debido a un proceso de autenticación inadecuado;
- acceso a información privilegiada, debido a falta de autorización;
- ejecución de comandos arbitrarios con privilegios innecesariamente elevados;
- carga y ejecución de archivos arbitrarios potencialmente dañinos sin restricción;
- divulgación de archivos confidenciales o ejecución de archivos maliciosos cargados, debido a un acceso a rutas no controlado (*path traversal*);
- ejecución de comandos no autorizados;
- ejecución de código malicioso en el navegador a través de un XSS;
- recuperación de credenciales, debido a una protección inadecuada de las mismas.

Para las vulnerabilidades se severidad alta y media, se han reservado los identificadores: CVE-2020-14484, CVE-2020-14494, CVE-2020-14491, CVE-2020-14493, CVE-2020-14488, CVE-2020-14490, CVE-2020-14486, CVE-2020-14492 y CVE-2020-14489.

Etiquetas: Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

---

Múltiples vulnerabilidades en CIM 500 de Grundfos Pumps Corporation

Fecha de publicación: 08/07/2020

Importancia: Alta

Recursos afectados:

CIM 500, todas las versiones de *firmware* anteriores a 06.16.00.

Descripción:

Marcin Dudek, de CERT.PL, reportó dos vulnerabilidades a CISA, ambas de severidad alta, de tipo falta de autenticación para función crítica y almacenamiento de credenciales desprotegido.

Solución:

Actualizar el *firmware* a la versión 06.16.00 y cambiar las credenciales de usuario después de la actualización.

Detalle:

- El producto afectado responde a solicitudes no autenticadas de archivos de almacenamiento de contraseña. Se ha reservado el identificador CVE-2020-10605 para esta vulnerabilidad.
- El producto afectado almacena credenciales de texto sin formato, lo que podría permitir la lectura de información confidencial o que alguien con acceso al dispositivo pudiera modificar la configuración del sistema. Se ha reservado el identificador CVE-2020-10609 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en Mitsubishi Electric GOT2000

Fecha de publicación: 08/07/2020

Importancia: Crítica

Recursos afectados:

GOT2000 CoreOS, versión -Y y anteriores, modelos GT23, GT25 y GT27.

Descripción:

El PSIRT de Mitsubishi Electric informó al CISA de estas vulnerabilidades que podrían permitir a un atacante remoto la denegación de servicio o la ejecución remota de código.

Solución:

Mitsubishi recomienda a los usuarios que sigan los siguientes pasos para actualizar el CoreOS a la última versión:

- Instalar MELSOFT GT Designer3 (2000), versión 1.240A o posterior en su ordenador personal.
- Iniciar MELSOFT GT Designer3 y copiar el CoreOS de la versión -Z o posterior a la tarjeta SD.
- Insertar la tarjeta SD extraída del ordenador personal en los productos afectados y actualizar a la última versión del CoreOS.

Detalle:

Las vulnerabilidades podrían permitir a un atacante:

- Bloquear el dispositivo, lo que podría conducir a la ejecución remota de código. Se ha asignado el identificador CVE-2020-5595 para esta vulnerabilidad.
- Causar una denegación de servicio de la conexión TCP. Se ha asignado el identificador CVE-2020-5596 para esta vulnerabilidad.
- Provocar una condición de denegación de servicio y bloquear el dispositivo. Se ha asignado el identificador CVE-2020-5597 para esta vulnerabilidad.
- Acceder a recursos sensibles, provocar una condición de denegación de servicio y bloquear el dispositivo. Se ha asignado el identificador CVE-2020-5598 para esta vulnerabilidad.
- Provocar una condición de denegación de servicio. Se ha asignado el identificador CVE-2020-5599 para esta vulnerabilidad.
- Obtener información confidencial. Se ha asignado el identificador CVE-2020-5600 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad XML External Entity (XEE) en Studio 5000 Logix Designer de Rockwell Automation

Fecha de publicación: 09/07/2020

Importancia: Baja

Recursos afectados:

Logix Designer Studio 5000, versiones 32.00, 32.01 y 32.02.

Descripción:

Durante la competición Pwn2Own, se hizo pública una vulnerabilidad en Logix Designer Studio 5000 que podría permitir a un atacante parsear un archivo malicioso, lo que podría dar lugar a la divulgación de información.

Solución:

Se recomienda que todos los clientes de Rockwell Automation que utilizan archivos AML o RDF no acepten archivos de fuentes desconocidas y sean cautelosos con los intentos de ingeniería social que puedan aprovecharse de esta vulnerabilidad.

Detalle:

Las versiones 32.00, 32.01 y 32.02 de Logix Designer Studio 5000 utilizan un analizador XML de terceros que acepta de forma nativa archivos AML y RDF de cualquier entidad externa. Si se explota con éxito, un atacante no autenticado podría ser capaz de crear un archivo malicioso, que al ser analizado, podría llevar a la divulgación de información de nombres de host u otros recursos del programa. Se ha reservado el identificador CVE-2020-12025 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Validación de entrada incorrecta en APM Connect de GE

Fecha de publicación: 10/07/2020

Importancia: Crítica

Recursos afectados:

APM Connect UDLP, versiones 2.8 y anteriores.

Descripción:

GE ha reportado una vulnerabilidad denominada *Ghostcat*, de severidad crítica, de tipo validación de entrada incorrecta, que afecta a varias versiones de su producto APM Connect UDLP.

Solución:

Aplicar las acciones indicadas en el apartado *Solution* del aviso de GE.

Detalle:

El riesgo asociado con esta vulnerabilidad es que un atacante podría ejecutar código malicioso y obtener acceso a información potencialmente confidencial, contenida en los archivos de configuración y archivos de código fuente de todas las aplicaciones web que dependen de Apache Tomcat. Se ha asignado el identificador CVE-2020-1938 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en MGate 5105-MB-EIP Series de Moxa

Fecha de publicación: 13/07/2020

Importancia: Alta

Recursos afectados:

MGate 5105-MB-EIP Series, versiones de *firmware* 4.2 o anteriores.

Descripción:

Los investigadores, Philippe Lin, Marco Balduzzi, Luca Bongiorni, Ryan Flores, Charles Perine y Rainer Vosseler, en colaboración con Zero Day Initiative de Trend Micro, han reportado dos vulnerabilidades de tipo omisión de autenticación por captura-repetición y exposición de información confidencial a un usuario no autorizado.

Solución:

1. Actualizar a la última versión de *firmware* disponible.
2. Deshabilitar la opción *Moxa Command* en la consola de configuraciones.
3. Si es necesario mantener habilitada la opción *Moxa Command*, activar las siguientes medidas de seguridad:
    - Habilitar *Apply additional restrictions* para evitar que un equipo no autorizado acceda al producto afectado.
    - Agregar la dirección IP del equipo a la lista de direcciones IP permitidas.

Detalle:

- Esta vulnerabilidad permitiría que un atacante obtuviese la ID de sesión de la conexión entre el *host* y el dispositivo. Se ha reservado el identificador CVE-2020-15494 para esta vulnerabilidad.
- Esta vulnerabilidad permitiría que un atacante descifrase el archivo de configuración cifrado del dispositivo. Se ha reservado el identificador CVE-2020-15493 para esta vulnerabilidad.

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

---

Boletín de seguridad de Siemens de julio de 2020

Fecha de publicación: 13/07/2020

Importancia: Crítica

Recursos afectados:

- SIMATIC HMI Basic Panels 1st Generation (variantes SIPLUS incluidas), todas las versiones;
- SIMATIC HMI Basic Panels 2nd Generation (variantes SIPLUS incluidas), todas las versiones;
- SIMATIC HMI Comfort Panels (variantes SIPLUS incluidas), todas las versiones;
- SIMATIC HMI KTP700F Mobile Arctic, todas las versiones;
- SIMATIC HMI Mobile Panels 2nd Generation, todas las versiones;
- SIMATIC WinCC Runtime Advanced, todas las versiones;
- Opcenter Execution Discrete, Opcenter Execution Foundation, Opcenter Execution Process, versiones anteriores a la 3.2;
- Opcenter Intelligence, todas las versiones;
- Opcenter Quality, versiones anteriores a la 11.3;
- Opcenter RD&L v8.0;
- SIMATIC IT LMS, todas las versiones;
- SIMATIC IT Production Suite, todas las versiones;
- SIMATIC Notifier Server for Windows, todas las versiones;
- SIMATIC PCS neo, todas las versiones;
- LOGO! 8 BM (variantes SIPLUS incluidas), versiones V1.81.01 - V1.81.03, V1.82.01 y V1.82.02;
- SPPA-T3000 Application Server, SPPA-T3000 Terminal Server, SPPA-T3000 APC UPS con tarjeta NMC, AP9630 o AP9631;
- Camstar Enterprise Platform, todas las versiones;
- Opcenter Execution Core, versiones anteriores a la 8.2;
- SICAM MMU, todas las versiones anteriores a la 2.05;
- SICAM SGU, todas las versiones;
- SICAM T, todas las versiones anteriores a la 2.18;
- SIMATIC S7-200, familia SMART CPU, todas las versiones, desde la V2.2, hasta la V2.5.1.

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 hay que 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 19 avisos de seguridad, de las cuales 12 son actualizaciones.

El tipo de nuevas vulnerabilidades publicadas se corresponde a los siguientes:

- 1 vulnerabilidad de transmisión de información sensible en texto claro,
- 1 vulnerabilidades de ruta de búsqueda o elemento sin entrecomillar,
- 2 vulnerabilidades de copia de búfer sin comprobación del tamaño de entrada (desbordamiento de búfer),
- 1 vulnerabilidad de manejo inadecuado de la longitud de los parámetros,
- 1 vulnerabilidad de desbordamiento o ajuste de enteros,
- 2 vulnerabilidades de neutralización incorrecta de la entrada durante la generación de la página web (Cross-site Scripting),
- 1 vulnerabilidad de neutralización incorrecta de elementos especiales usados en un comando SQL (inyección SQL),
- 1 vulnerabilidad de lectura fuera de límites,
- 2 vulnerabilidades de ausencia de autenticación para una función crítica,
- 1 vulnerabilidad de ausencia de cifrado en información sensible,
- 1 vulnerabilidad de uso de hash de contraseña generado con esfuerzo computacional insuficiente,
- 1 vulnerabilidad de neutralización inadecuada de etiquetas HTML relacionadas con scripts en una página web (XSS básico),
- 1 vulnerabilidad de omisión de autenticación mediante *capture-replay*,
- 1 vulnerabilidad de consumo de recursos no controlado (agotamiento de recursos).

Para estas vulnerabilidades se han reservado los siguientes identificadores: CVE-2020-7592, CVE-2020-7581, CVE-2020-7587, CVE-2020-7588, CVE-2020-7593, CVE-2020-11896, CVE-2020-0545, CVE-2020-7576, CVE-2020-7577, CVE-2020-7578, CVE-2020-10037, CVE-2020-10038, CVE-2020-10039, CVE-2020-10040, CVE-2020-10041, CVE-2020-10042, CVE-2020-10043, CVE-2020-10044, CVE-2020-

10045CVE-2020-10045 y CVE-2020-7584.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en Advantech iView

Fecha de publicación: 15/07/2020

Importancia: Crítica

Recursos afectados:

iView, versiones 5.6 y anteriores.

Descripción:

Se han publicado múltiples vulnerabilidades, 3 de severidad crítica y 3 altas, que podrían permitir a un atacante leer o modificar información, ejecutar código arbitrario, limitar la disponibilidad del sistema o provocar el cierre inesperado de la aplicación.

Solución:

Actualizar a la versión 5.7.

Detalle:

- Múltiples vulnerabilidades de inyección SQL podrían permitir a un atacante extraer las credenciales del usuario, leer o modificar la información o ejecutar código de forma remota. Se ha asignado el identificador CVE-2020-14497 para esta vulnerabilidad.
- Vulnerabilidades de salto de ruta (path traversal) podrían permitir a un atacante crear/descargar archivos arbitrarios, limitar la disponibilidad del sistema o ejecutar código de forma remota. Se ha asignado el identificador CVE-2020-14507 para esta vulnerabilidad.
- La neutralización incorrecta de los elementos especiales podría permitir a un atacante enviar una solicitud HTTP GET o POST que crea una cadena de comandos sin ninguna validación. El atacante podría entonces ejecutar código remotamente. Se ha asignado el identificador CVE-2020-14505 para esta vulnerabilidad.
- La validación inadecuada de los datos de entrada podría permitir a un atacante la ejecución remota de código arbitrario. Se ha asignado el identificador CVE-2020-14503 para esta vulnerabilidad.
- La falta de autenticación para una función crítica podría permitir a un atacante obtener la información de la tabla de usuarios, incluidas las credenciales de administrador en texto plano o eliminar la cuenta de administrador. Se ha asignado el identificador CVE-2020-14501 para esta vulnerabilidad.
- El control de acceso inadecuado podría permitir a un atacante obtener todas las credenciales de las cuentas de usuario. Se ha asignado el identificador CVE-2020-14499 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Schneider Electric

Fecha de publicación: 15/07/2020

Importancia: Alta

Recursos afectados:

- Schneider Electric Software Update (SESU) V2.4.0 y anteriores.
- Schneider Electric Floating License Manager V2.4.0.0 y anteriores.

Ambos productos de software son utilizados en múltiples productos de Schneider Electric. Se recomienda revisar la sección de Referencias para conocer el listado completo en los que se usan estos programas.

Descripción:

Schneider Electric ha reportado varias vulnerabilidades en sus productos que permitirían la ejecución remota de código o una denegación de servicio en los productos afectados.

Solución:

Schneider Electric ha publicado las siguientes versiones que corrigen estas vulnerabilidades:

- Schneider Electric Software Update (SESU) V2.5.0.
- Schneider Electric Floating License Manager V2.5.0.0.

Detalle:

La vulnerabilidad encontrada en Schneider Electric Software Update (SESU) permitiría a un atacante, mediante la redirección de una URL, ejecutar código en el equipo de la víctima. Se requiere acceso al equipo de la víctima para manipular una clave de registro de Windows para utilizar esta vulnerabilidad.

Las vulnerabilidades encontradas en Schneider Electric Floating License Manager están relacionadas con el manejo de comandos y con el agotamiento de memoria para la pila en FlexNet a través de lmadmin.exe versión 11.16.2, provocando en ambos casos una denegación de servicio.

Se han asignado los siguientes identificadores para estas vulnerabilidades: CVE-2020-7520, CVE-2019-8960 y CVE-2019-8961

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

---

Ejecución remota de código en eCatcher de eWON

Fecha de publicación: 16/07/2020

Importancia: Crítica

Recursos afectados:

eCatcher, versiones anteriores a 6.5.5.

Descripción:

La compañía de ciberseguridad Claroty ha notificado a HMS una vulnerabilidad, de severidad crítica, de tipo ejecución remota de código (RCE), que afecta a su producto eCatcher.

Solución:

HMS recomienda que eCatcher se actualice a la versión 6.5.5 o superiores para solucionar esta vulnerabilidad.

Detalle:

Un atacante, remoto, podría aprovechar esta vulnerabilidad para realizar una ejecución remota de código (RCE) en la aplicación eCatcher, el *software* de acceso remoto de Talk2M con el que se puede gestionar la cuenta de Talk2M y conectarse a todos los dispositivos situados en la LAN del eWON.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad en PLCnext Engineer de Phoenix Contact

Fecha de publicación: 22/07/2020

Importancia: Alta

Recursos afectados:

PLCnext Engineer (1046008) 2020.3.1 y anteriores

Descripción:

 ha publicado una vulnerabilidad del tipo limitación incorrecta de nombre de ruta a un directorio restringido (Path Traversal) en productos Phoenix Contact que podría permitir a un atacante la ejecución remota de código.

Solución:

Actualizar a PLCnext Enineer 2020.6 o superior.

Detalle:

Los parámetros de construcción de un proyecto de PLCnext Engineer (.pcwex) pueden ser manipulados por un atacante con acceso al proyecto, lo que podría permitir la ejecución remota de código. Se ha asignado el identificador CVE-2020-12499 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Asignación de memoria no controlada en CODESYS V3 Visualization

Fecha de publicación: 23/07/2020

Importancia: Alta

Recursos afectados:

Todos los sistemas en tiempo de ejecución de CODESYS V3, en todas las versiones anteriores a la V3.5.16.10, están afectados, los cuales soportan el CODESYS Target-o Webvisualization y contienen CmpVisuServer y CmpVisuHandler, independientemente del tipo de CPU o sistema operativo:

- CODESYS Control para BeagleBone,
- CODESYS Control para emPC-A/iMX6,
- CODESYS Control para IOT2000,
- CODESYS Control para Linux,
- CODESYS Control para Linux ARM,
- CODESYS Control para PLCnext,
- CODESYS Control para PFC100,
- CODESYS Control para PFC200,
- CODESYS Control para Raspberry Pi,
- CODESYS Control para WAGO Touch Panels 600,
- CODESYS Control RTE V3,
- CODESYS Control RTE V3 (para Beckhoff CX),
- CODESYS Control Win V3 (también parte de CODESYS Development System setup),
- CODESYS V3 Simulation Runtime (parte de CODESYS Development System),
- CODESYS HMI V3,
- CODESYS Control V3 Runtime System Toolkit,

- CODESYS V3 Embedded Target Visu Toolkit,
- CODESYS V3 Remote Target Visu Toolkit.

Descripción:

La vulnerabilidad publicada podría permitir a un atacante remoto agotar la memoria del sistema y provocar su bloqueo.

Solución:

Actualizar a la versión V3.5.16.10.

Detalle:

Las máscaras de visualización creadas en CODESYS se muestran con la ayuda de algunos componentes del sistema de tiempo de ejecución de CODESYS Control, que procesan las solicitudes para mostrarlas en la pantalla. Un atacante remoto que envíe solicitudes específicamente diseñadas al sistema de tiempo de ejecución de CODESYS Control, podría provocar la asignación arbitraria de cantidades de memoria, haciendo que el sistema se quede sin memoria y se bloquee. Se ha asignado el identificador CVE-2020-15806 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Triconex de Schneider

Fecha de publicación: 24/07/2020

Importancia: Crítica

Recursos afectados:

Las siguientes versiones antiguas de sistemas Triconex:

- TriStation 1131, v1.0.0 a v4.9.0, v4.10.0, y 4.12.0, operando en Windows NT, Windows XP, o Windows 7;
- Módulo de Comunicaciones Tricon (TCM), modelos 4351, 4352, 4351A/B y 4352A/B instalado en sistemas Tricon v10.0 a v10.5.3.

Los usuarios de las versiones actuales y más recientes del firmware y el software identificados no están expuestos a estas vulnerabilidades específicas.

Descripción:

Schneider ha publicado una vulnerabilidad en versiones muy antiguas de productos Triconex que podría permitir a un atacante ver datos en texto claro en la red, provocar una condición de denegación de servicio o realizar un acceso indebido.

Solución:

Actualizar a las versiones recientes:

- TriStation v4.9.1, v4.10.1, v4.13.0 o v10.5.4.

Detalle:

- Una vulnerabilidad relacionada con la función de 'contraseña' de TriStation 1131, versiones 1.0 a 4.12.0, podría hacer que ciertos datos fueran visibles en la red cuando esta se habilitara. Se ha asignado el identificador CVE-2020-7483 para esta vulnerabilidad.
- Una vulnerabilidad relacionada con la característica de 'contraseña' en TriStation 1131, versiones 1.0 a 4.12.0, podría permitir un ataque de denegación de servicio si el usuario no está siguiendo las directrices documentadas relativas a la conexión dedicada de la TriStation 1131 y la protección *key-switch*. Se ha asignado el identificador CVE-2020-7484 para esta vulnerabilidad.
- Una vulnerabilidad relacionada con una cuenta de soporte en las versiones 1.0 a 4.9.0 y 4.10.0, de TriStation 1131, podría permitir un acceso inapropiado al archivo del proyecto TriStation 1131. Se ha asignado el identificador CVE-2020-7485 para esta vulnerabilidad.
- Una vulnerabilidad podría causar que los TCMs instalados en el sistema Tricon, versiones 10.0.0 a 10.4.x, se reinicien cuando se encuentren bajo una alta carga de la red. Este reinicio podría resultar en un comportamiento de negación de servicio con el SIS. Se ha asignado el identificador CVE-2020-7486 para esta vulnerabilidad.
- Una cuenta de puerto de depuración en TCMs instaladas en el sistema Tricon, versiones 10.2.0 a 10.5.3, es visible en la red, lo que podría permitir un acceso inapropiado. Se ha asignado el identificador CVE-2020-7491 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Softing Industrial Automation OPC

Fecha de publicación: 29/07/2020

Importancia: Crítica

Recursos afectados:

Todas las versiones de OPC anteriores al último *build* de la versión 4.7.0.

Descripción:

El investigador, Uri Katz, de Claroty, reportó 2 vulnerabilidades al CISA, una con severidad crítica y otra alta, de tipo desbordamiento de búfer basado en montículo (*heap*) y consumo descontrolado de recursos, que afectan a OPC de Softing Industrial Automation.

Solución:

Softing Industrial Automation ha publicado una actualización para mitigar las vulnerabilidades reportadas. La versión más actualizada, en

el momento de este aviso de CISA, se puede encontrar en el sitio web de Softing Industrial Automation.

Detalle:

- El producto afectado es vulnerable a un desbordamiento de búfer basado en montículo (*heap*), lo que podría permitir que un atacante ejecutase código arbitrario de forma remota. Se ha reservado el identificador CVE-2020-14524 para esta vulnerabilidad.
- El producto afectado es vulnerable a un consumo incontrolado de recursos, lo que podría permitir que un atacante provocase una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2020-14522 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en GateManager de Secomea

Fecha de publicación: 29/07/2020

Importancia: Crítica

Recursos afectados:

GateManager, servidor VPN, versiones anteriores a la 9.2c.

Descripción:

Sharon Brizinov y Tal Keren, de Claroty, han reportado al CISA vulnerabilidades que podrían permitir a un atacante enviar un valor negativo y sobrescribir datos arbitrarios, ejecutar código arbitrario de manera remota, provocar la denegación del servicio, ejecutar comandos como *root* o visualizar contraseñas.

Solución:

Actualizar a las últimas versiones, disponibles en la página web de Secomea.

Detalle:

- La neutralización incorrecta de los caracteres o los bytes *null* podría permitir a un atacante enviar un valor negativo o sobreescribir información arbitraria. Se ha reservado el identificador CVE-2020-14500 para esta vulnerabilidad.
- Un error *off-by-one* podría permitir a un atacante remoto ejecutar código arbitrario o provocar la denegación del servicio. Se ha reservado el identificador CVE-2020-14508 para esta vulnerabilidad.
- La utilización de contraseñas embebidas podría permitir a un atacante ejecutar comandos como *root*. Se ha reservado el identificador CVE-2020-14510 para esta vulnerabilidad.
- La utilización de *hash* de contraseñas débiles podría permitir a un atacante ver contraseñas de usuario. Se ha reservado el identificador CVE-2020-14512 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad en DreamMapper de Philips

Fecha de publicación: 31/07/2020

Importancia: Media

Recursos afectados:

DreamMapper, versión 2.24 y anteriores.

Descripción:

Se ha publicado una vulnerabilidad del tipo información sensible presente en archivos de log que podría permitir a un atacante acceder a la descripción detallada de los diferentes tipos de mensajes de error.

Solución:

Está prevista una actualización de DreamMapper para julio de 2021.

Para cualquier duda, contactar con el servicio de soporte de Philips.

Detalle:

La información escrita en los ficheros de log pueden servir de guía a un atacante, ya que podría acceder a la descripción detallada de los diferentes tipos de mensajes de error. Se ha reservado el identificador CVE-2020-14518 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

---

Múltiples vulnerabilidades en varios productos de Mitsubishi Electric

Fecha de publicación: 31/07/2020

Importancia: Alta

Recursos afectados:

- C Controller Interface Module Utility, todas las versiones;
- C Controller Module Setting y Monitoring Tool, todas las versiones;
- CC-Link IE Control Network Data Collector, todas las versiones;
- CC-Link IE Field Network Data Collector, todas las versiones;
- CPU Module Logging Configuration Tool, versión 1.100E y anteriores;
- CW Configurator, versión 1.010L y anteriores;
- Data Transfer, todas las versiones;
- EZSocket, todas las versiones;
- FR Configurator SW3, todas las versiones;
- FR Configurator2, todas las versiones;
- GT Designer2 Classic, todas las versiones;
- GT Designer3 Version1 (GOT1000), todas las versiones;
- GT Designer3 Version1 (GOT2000), todas las versiones;
- GT SoftGOT1000 Version3, todas las versiones;
- GT SoftGOT2000 Version1, todas las versiones;
- GX Developer, versiones 8.504A y anteriores,
- GX LogViewer, versión 1.100E y anteriores;
- GX Works2, todas las versiones;
- GX Works3, versión 1.063R y anteriores;
- Herramientas de configuración / monitorización para el módulo C Controller, todas las versiones;
- M_CommDTM-HART, versión 1.00A;
- M_CommDTM-IO-Link, todas las versiones;
- MELFA-Works, todas las versiones;
- MELSEC WinCPU Setting Utility, todas las versiones;
- MELSEC iQ-R Series Motion Module, todas las versiones;
- MELSOFT iQ AppPortal, todas las versiones;
- MELSOFT EM Software Development Kit (EM Configurator), todas las versiones;
- MELSOFT FieldDeviceConfigurator, versión 1.03D y anteriores;
- MELSOFT Navigator, todas las versiones;
- MELSOFT Complete Clean Up Tool, todas las versiones;
- MH11 SettingTool Version2, versión 2.002C y anteriores;
- MI Configurator, todas las versiones;
- Motion Control Setting, versión 1.005F y anteriores;
- Motorizer, versión 1.005F y anteriores;
- MR Configurator2, todas las versiones;
- MT Works2, todas las versiones;
- MTConnect Data Collector, todas las versiones;
- MX Component, todas las versiones;
- MX MESInterface, todas las versiones;
- MX MESInterface-R, todas las versiones;
- MX Sheet, todas las versiones;
- Network Interface Board CC IE Control utility, todas las versiones;
- Network Interface Board CC IE Field Utility, todas las versiones;
- Network Interface Board CC-Link Ver.2 Utility, todas las versiones;
- Network Interface Board MNETH utility, todas las versiones;
- Position Board utility 2, todas las versiones;
- PX Developer, todas las versiones;
- RT ToolBox2, todas las versiones;
- RT ToolBox3, todas las versiones;
- SLMP Data Collector, todas las versiones.

Descripción:

El equipo de investigación de Applied Risk, junto con los investigadores, Younes Dragoni, de Nozomi Networks, y Mashav Sapir, de Claroty, han reportado al CISA 3 vulnerabilidades, todas con severidad alta, de tipo problemas de permisos, acceso a rutas no controlado (*path traversal*) y ruta de búsqueda o elemento sin entrecomillar.

Solución:

Descargar la última versión de *software* de cada producto afectado.

Detalle:

- La explotación exitosa de esta vulnerabilidad podría permitir a un atacante escalar privilegios y ejecutar programas maliciosos, lo que podría causar una condición de denegación de servicio (DoS) o permitir que la información sea revelada, manipulada y/o destruida. Se ha reservado el identificador CVE-2020-14496 para esta vulnerabilidad.
- Varios productos de Mitsubishi Electric Factory Automation tienen una vulnerabilidad que podría permitir a un atacante ejecutar código arbitrario. Se ha reservado el identificador CVE-2020-14523 para esta vulnerabilidad.
- Varios productos de ingeniería de *software* de Mitsubishi Electric Factory Automation contienen una vulnerabilidad de ejecución de código malicioso. Un atacante malintencionado podría usar esta vulnerabilidad para obtener información, modificar información o causar una condición de denegación de servicio (Dos). Se ha reservado el identificador CVE-2020-14521 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en varios productos de Yokogawa

Fecha de publicación: 31/07/2020

Importancia: Alta

Recursos afectados:

- CENTUM CS 3000 R3.08.10 - R3.09.50 (incluyendo CENTUM CS 3000 Entry Class);
- CENTUM VP R4.01.00 - R6.07.00 (incluyendo CENTUM VP Entry Class);
- B/M9000CS R5.04.01 - R5.05.01;
- B/M9000 VP R6.01.01 - R8.03.01.

Descripción:

Nataliya Tlyapova e Ivan Kurnakov, investigadores de Positive Technologies, han notificado a Yokogawa dos vulnerabilidades, ambas con severidad alta, de tipo autenticación inadecuada y acceso a rutas no controlado (*path traversal*).

Solución:

- CENTUM CS 3000 R3.08.10 - R3.09.50: este producto está discontinuado y no dispondrá de parche para corregir las vulnerabilidades, se recomienda actualizar a la última versión de CENTUM VP.
- CENTUM VP:
  - R4.01.00 - R4.03.00: estas versiones del producto están discontinuadas y no dispondrán de parche para corregir las vulnerabilidades, se recomienda actualizar a la última versión de CENTUM VP;
  - R5.01.00 - R5.04.20: actualizar a la última versión disponible (R5.04.20) y aplicar el parche (R5.04.D1);
  - R6.01.00 - R6.07.00: actualizar a la última versión disponible (R6.07.00) y aplicar el parche (R6.07.11).
- B/M9000CS R5.04.01 - R5.05.01: este producto no se ve afectado por las vulnerabilidades, pero sí por la existencia de CENTUM CS 3000 instalado en el mismo equipo. Si se necesita actualizar CENTUM CS 3000, también se debe actualizar B/M9000CS a la revisión adecuada.
- B/M9000 VP R6.01.01 - R8.03.01: este producto no se ve afectado por las vulnerabilidades, pero sí por la existencia de CENTUM VP instalado en el mismo equipo. Si se necesita actualizar CENTUM VP, también se debe actualizar B/M9000 VP a la revisión adecuada.

Detalle:

- Esta vulnerabilidad podría permitir que un atacante remoto, no autenticado, enviase paquetes de comunicación especialmente diseñados. Se ha reservado el identificador CVE-2020-5608 para esta vulnerabilidad.
- Esta vulnerabilidad podría permitir a un atacante remoto crear o sobrescribir cualquier archivo, o ejecutar cualquier comando. Se ha reservado el identificador CVE-2020-5609 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad