Boletín de septiembre de 2020

Avisos de Sistemas de Control Industrial

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Suplantación de un dispositivo legítimo en varios productos de Mitsubishi Electric

Fecha de publicación: 02/09/2020

Importancia: Alta

Recursos afectados:

- QJ71MES96, todas las versiones;
- QJ71WS96, todas las versiones;
- Q06CCPU-V, todas las versiones;
- Q24DHCCPU-V, todas las versiones;
- Q24DHCCPU-VG, todas las versiones;
- R12CCPU-V, todas las versiones;
- RD55UP06-V, todas las versiones;
- RD55UP12-V, todas las versiones;
- RJ71GN11-T2, todas las versiones;
- RJ71EN71, todas las versiones;
- QJ71E71-100, todas las versiones;
- LJ71E71-100, todas las versiones;
- QJ71MT91, todas las versiones;
- RD78Gn(n=4,8,16,32,64), todas las versiones;
- RD78GHV, todas las versiones;
- RD78GHW, todas las versiones;
- NZ2GACP620-60, todas las versiones;
- NZ2GACP620-300, todas las versiones;
- NZ2FT-MT, todas las versiones;
- NZ2FT-EIP, todas las versiones;
- Q03UDECPU, los primeros 5 dígitos del número de serie 22081 y anteriores;
- QnUDEHCPU(n=04/06/10/13/20/26/50/100), los primeros 5 dígitos del número de serie 22081 y anteriores;
- QnUDVCPU(n=03/04/06/13/26), los primeros 5 dígitos del número de serie 22031 y anteriores;
- QnUDPVCPU(n=04/06/13/2), los primeros 5 dígitos del número de serie 22031 y anteriores;

- LnCPU(-P)(n=02/06/26), los primeros 5 dígitos del número de serie 22051 y anteriores;
- L26CPU-(P)BT, los primeros 5 dígitos del número de serie 22051 y anteriores;
- RnCPU(n=00/01/02), versión 18 y anteriores;
- RnCPU(n=04/08/16/32/120), versión 50 y anteriores;
- RnENCPU(n=04/08/16/32/120), versión 50 y anteriores;
- RnSFCPU (n=08/16/32/120), todas las versiones;
- RnPCPU(n=08/16/32/120), todas las versiones;
- RnPSFCPU(n=08/16/32/120), todas las versiones;
- FX5U(C)-**M*/**
  - Caso 1: número de serie 17X**** o posteriores: versión 1.210 y anteriores;
  - Caso 2: número de serie 179**** y anteriores: versión 1.070 y anteriores;
- FX5UC-32M*/**-TS, versión 1.210 y anteriores;
- FX5UJ-**M*/**, versión 1.000;
- FX5-ENET, todas las versiones;
- FX5-ENET/IP, todas las versiones;
- FX3U-ENET-ADP, todas las versiones;
- FX3GE-**M*/**, todas las versiones;
- FX3U-ENET, todas las versiones;
- FX3U-ENET-L, todas las versiones;
- FX3U-ENET-P502, todas las versiones;
- FX5-CCLGN-MS, todas las versiones;
- IU1-1M20-D, todas las versiones;
- LE7-40GU-L, todas las versiones;
- GOT2000 Series GT21 Model, todas las versiones;
- GS Series, todas las versiones;
- GOT1000 Series GT14 Model, todas las versiones;
- GT25-J71GN13-T2, todas las versiones;
- FR-A800-E Series, todas las versiones;
- FR-F800-E Series, todas las versiones;
- FR-A8NCG, fecha de producción de agosto 2020 y anteriores;
- FR-E800-EPA Series, fecha de producción de julio 2020 y anteriores;
- FR-E800-EPB Series, fecha de producción de julio 2020 y anteriores;
- Conveyor Tracking Application APR-nTR3FH, APR-nTR6FH, APR-nTR12FH, APR-nTR20FH(n=1,2), todas las versiones (producto discontinuado);
- MR-JE-C, todas las versiones;
- MR-J4-TM, todas las versiones.

Descripción:

Ta-Lun Yen, de TXOne IoT/ICS Security Research Labs de Trend Micro, en colaboración con Zero Day Initiative de Trend Micro, ha informado de una vulnerabilidad, con severidad alta, de suplantación de un dispositivo legítimo que afecta a múltiples productos de Mitsubishi Electric.

Solución:

Mitsubishi Electric recomienda que los usuarios adopten las siguientes medidas para minimizar el riesgo de esta vulnerabilidad:

- Recomendaciones generales de seguridad: utilizar *firewall*, VPN, LAN y antivirus actualizado.
- RnCPU (n = 00/01/02), versión 18 y anteriores: actualizar a la versión 19 o posterior;
- RnCPU (n = 04/08/16/32/120), versión 50 y anteriores: actualizar a la versión 51 o posterior;
- RnENCPU (n = 04/08/16/32/120), versión 50 y anteriores: actualizar a la versión 51 o posterior;
- FX5U (C) - ** M * / **
  - Caso 1: número de serie 17X **** o posterior, versión 1.210 y anterior: actualizar a la versión 1.211 o posterior;
  - Caso 2: número de serie 179 **** y anterior, versión 1.070 y anterior: actualizar a la versión 1.071 o posterior;
- FX5UC-32M * / ** - TS, versión 1.210 y anteriores: actualizar a la versión 1.211 o posterior;
- FX5UJ - ** M * / **, versión 1.000: actualizar a la versión 1.001 o posterior.

Detalle:

Los productos afectados son vulnerables a la suplantación de un dispositivo legítimo por parte de un atacante, lo que podría permitir que dicho atacante ejecutase comandos arbitrarios de forma remota. Se ha reservado el identificador CVE-2020-16226 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Avisos de seguridad de Siemens de septiembre de 2020

Fecha de publicación: 08/09/2020

Importancia: Crítica

Recursos afectados:

- Information Server, 2019 SP1 y posteriores;
- License Management Utility (LMU), todas las versiones anteriores a la V2.4;
- Polarion Subversion Webclient, todas las versiones;
- Process Historian (incluido Process Historian OPC UA Server), versión 2019 y posteriores;
- SIMATIC Field PG M4, Field PG M5 y Field PG M6, todas las versiones;
- SIMATIC HMI Basic Panels 2nd Generation (incluidas las variantes SIPLUS), todas las versiones superiores o iguales a la 14 y anteriores a la XX;

- SIMATIC HMI Basic Panels 2nd Generation (incluidas las variantes SIPLUS), todas las versiones;
- SIMATIC HMI Mobile Panels, todas las versiones;
- SIMATIC HMI United Comfort Panels, todas las versiones;
- SIMATIC IPC3000 SMART, IPC347E, IPC427D (incluidas las variantes SIPLUS), IPC427E (incluidas las variantes SIPLUS), IPC477D, IPC477E, IPC477E Pro, IPC527G, IPC547E, IPC547G, IPC627D, IPC627E, IPC647D, IPC647E, IPC677D, IPC677E, IPC827D, PC847D, IPC847E, ITP1000, todas las versiones;
- SIMATIC PCS neo, todas las versiones;
- SIMATIC RTLS Locating Manager, todas las versiones anteriores a la V2.10.2;
- SIMATIC S7-300 CPU family (incluido ET200 CPUs y las variantes SIPLUS), todas las versiones;
- SIMATIC S7-400 CPU family (incluidas variantes SIPLUS), todas las versiones;
- SIMATIC WinCC OA, versión V3.17;
- SIMIT Simulation Platform, versión V10.0 y posteriores;
- SIMOTION P320-4E y P320-4S, todas las versiones;
- SINEC INS, todas las versiones;
- SINEMA Remote Connect, todas las versiones;
- SINUMERIK 828D (PPU.4 / PPU1740), SINUMERIK 840D sl (NCU730.3B), SINUMERIK ONE (NCU1750 / NCU1760);
- Siveillance Video Client, todas las versiones.
- Spectrum Power^{TM} 4, todas las versions anteriores a la V4.70 SP8;
- SPPA-S2000 (S7), versiones V3.04 y V3.06;
- SPPA-S3000, versiones V3.04 y V3.05;
- SPPA-T3000, versión R8.2 SP2;

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 los cuales 10 son actualizaciones.

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

- 1 vulnerabilidad de validación incorrecta de entrada;
- 1 vulnerabilidad de revelación de información;
- 1 vulnerabilidad de ejecución sin los privilegios necesarios;
- 2 vulnerabilidades de permisos por defecto incorrectos;
- 1 vulnerabilidad de elusión de autenticación;
- 1 vulnerabilidad de restricción inadecuada en los intentos fallidos de autenticación;
- 1 vulnerabilidad de almacenamiento de información sensible en texto claro;
- 1 vulnerabilidad de transmisión de información sensible en texto claro;
- 1 vulnerabilidad de fortaleza de cifrado inadecuada;
- 1 vulnerabilidad de error de validación del origen;
- 1 vulnerabilidad de verificación incorrecta de la firma criptográfica;
- 1 vulnerabilidad de falsificación de petición en sitios cruzados (Cross-Site Request Forgery);
- 1 vulnerabilidad de apagado o liberación incorrecto de recursos;
- 1 vulnerabilidad de ruta de búsqueda o elemento sin entrecomillar;
- 1 vulnerabilidad de credenciales insuficientemente protegidas;
- 1 vulnerabilidad de exposición de la información a través de la lista de directorios;
- 1 vulnerabilidad de neutralización inadecuada de etiquetas HTML relacionadas con scripts en una página web (XSS básico);
- 1 vulnerabilidad de acceso al búfer con un valor de longitud incorrecta.

Para estas vulnerabilidades se han reservado los siguientes identificadores: CVE-2020-10049, CVE-2020-10050, CVE-2020-10051, CVE-2020-15791, CVE-2020-15788, CVE-2020-15789, CVE-2020-14509, CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, CVE-2020-16233, CVE-2020-0543, CVE-2020-15786, CVE-2020-15787, CVE-2020-15784, CVE-2020-15790, CVE-2020-10056 y CVE-2020-15785.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en productos Schneider

Fecha de publicación: 09/09/2020

Importancia: Alta

Recursos afectados:

- SCADAPack 7x Remote Connect, versión V3.6.3.574 y anteriores;
- SCADAPack x70 Security Administrator, versión V1.2.0 y anteriores.

Descripción:

Schneider Electric ha publicado múltiples vulnerabilidades, 3 de severidad media y 2 altas, que afectan a sus productos SCADAPack 7x Remote Connect y a SCADAPack x70 Security Administrator y que podrían permitir la ejecución arbitraria de código, añadir contenido en carpetas no protegidas o acceder a las carpetas con código ejecutable.

Solución:

Actualizar a SCADAPack 7x RemoteConnect V3.7.3.904 y a SCADAPack x70 Security Administrator V1.6.2. Ambos disponibles como parte del paquete RemoteConnect V2.3.2.

Detalle:

- Una vulnerabilidad de deserialización de datos no confiables podría permitir la ejecución de código arbitrario cuando un atacante construye un archivo .PRJ especialmente diseñado que contiene un búfer serializado malicioso. Se ha asignado el identificador CVE-2020-7528 para esta vulnerabilidad de severidad media.
- Una vulnerabilidad de limitación inadecuada de una ruta de acceso a un directorio restringido ("path transversal") podría permitir a un atacante colocar contenido en cualquier carpeta no protegida del sistema de destino utilizando un archivo .RCZ especialmente diseñado. Se ha asignado el identificador CVE-2020-7529 para esta vulnerabilidad de severidad media.
- Una vulnerabilidad de autorización inadecuada podría permitir el acceso indebido a las carpetas de código ejecutable. Se ha asignado el identificador CVE-2020-7530 para esta vulnerabilidad de severidad alta.
- Una vulnerabilidad de control de acceso inapropiado podría permitir a un atacante colocar los ejecutables en una carpeta específica y ejecutar código siempre que el usuario ejecute RemoteConnect. Se ha asignado el identificador CVE-2020-7531 para esta vulnerabilidad de severidad media.
- Una vulnerabilidad de deserialización de datos no confiables podría permitir la ejecución de código arbitrario cuando un atacante construye un archivo .SDB especialmente diseñado que contiene un búfer serializado malicioso. Se ha asignado el identificador CVE-2020-7532 para esta vulnerabilidad de severidad alta.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Múltiples vulnerabilidades en Enterprise Data Management Web de AVEVA

Fecha de publicación: 09/09/2020

Importancia: Alta

Recursos afectados:

AVEVA Enterprise Data Management Web v2019 y todas las versiones anteriores conocidas como eDNAWeb.

Descripción:

AVEVA ha publicado múltiples vulnerabilidades de inyección de código SQL que podrían permitir a un atacante ejecutar comandos SQL arbitrarios.

Solución:

Actualizar a AVEVA™ Enterprise Data Management Web v2019 SP1, si esto no es posible, próximamente se lanzará un hotfix para eDNA Webv2018SP2.

Detalle:

Múltiples vulnerabilidades de neutralización incorrecta de elementos especiales usados en un comando SQL (inyección SQL) en eDNAWeb podrían permitir a un atacante ejecutar comandos SQL arbitrarios con los privilegios de la cuenta eDNA Web para accesos SQL.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en dispositivos de monitorización de pacientes de Philips

Fecha de publicación: 11/09/2020

Importancia: Alta

Recursos afectados:

- Patient Information Center iX (PICiX), versiones B.02, C.02, C.03;
- PerformanceBridge Focal Point, versión A.01;
- IntelliVue patient monitors MX100, MX400-MX850 y MP2-MP90, versiones N y anteriores;
- IntelliVue X3 y X2, versiones N y anteriores.

Descripción:

Se han publicado múltiples vulnerabilidades en dispositivos de monitorización de pacientes de Philips que podrían permitir a un atacante el acceso no autorizado a los datos del paciente, reiniciar la aplicación, cerrar el servicio de certificados de forma inesperada, reiniciar el sistema o salir del entorno restringido con privilegios limitados.

Solución:

Están previstas las siguientes actualizaciones:

- Patient Information Center iX (PICiX) Version C.03, para finales de 2020;
- PerformanceBridge Focal Point para el segundo cuatrimestre de 2021;
- IntelliVue Patient Monitors Versions N.00 and N.01 para el primer cuatrimestre de 2021;

- IntelliVue Patient Monitors Version M.04 para finales de 2021;
- El sistema de revocación de certificados será implementado en 2023.

Detalle:

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

- Neutralización incorrecta de elementos de fórmula en archivos CSV. Se ha asignado el identificador CVE-2020-16214 para esta vulnerabilidad.
- Neutralización incorrecta de la entrada durante la generación de la página web (Cross-site Scripting). Se ha asignado el identificador CVE-2020-16218 para esta vulnerabilidad.
- Autenticación incorrecta. Se ha asignado el identificador CVE-2020-16222 para esta vulnerabilidad.
- Comprobación inadecuada de la revocación de certificados. Se ha asignado el identificador CVE-2020-16228 para esta vulnerabilidad.
- Manejo inadecuado de la inconsistencia en la longitud de los parámetros. Se ha asignado el identificador CVE-2020-16224 para esta vulnerabilidad.
- Validación inadecuada del corrector sintáctico de los datos de entrada. Se ha asignado el identificador CVE-2020-16220 para esta vulnerabilidad.
- Validación incorrecta de entrada. Se ha asignado el identificador CVE-2020-16216 para esta vulnerabilidad.
- Exposición del recurso a una esfera de control incorrecta. Se ha asignado el identificador CVE-2020-16212 para esta vulnerabilidad.

Etiquetas: Actualización, Sanidad, Vulnerabilidad

Vulnerabilidad en FATEK Automation PLC WinProladder

Fecha de publicación: 11/09/2020

Importancia: Alta

Recursos afectados:

PLC WinProladder, versión 3.28 y anteriores.

Descripción:

Se han publicado múltiples vulnerabilidades en los PLC WinProladde que podrían permitir a un atacante colapsar el dispositivo al que se accede, denegar el servicio y la ejecución remota del código.

Solución:

Contactar con el servicio de soporte de Fatek.

Detalle:

La vulnerabilidad, del tipo desbordamiendo de búfer basado en pila (stack), puede ser explotada cuando un usuario abre un archivo especialmente diseñado, lo que podría permitir a un atacante la ejecución remota de código. Se ha asignado el identificador CVE-2020-10597 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en codificadores IPTV basados en hardware HiSilicon

Fecha de publicación: 16/09/2020

Importancia: Crítica

Recursos afectados:

Los fabricantes afectados por alguna de estas vulnerabilidades son:

- URayTech;
- J-Tech Digital;
- VeCASTER PRO de Pro Video Instruments.

Otras marcas aún no han sido confirmadas.

Descripción:

Se han publicado múltiples vulnerabilidades (4 críticas, 1 alta y 1 media) en varios dispositivos codificadores de vídeo sobre IP, también conocidos como codificadores de vídeo IPTV/H.264/H.265, que están basados en el hardware HiSilicon Hi3520d. Estas vulnerabilidades podrían permitir a un atacante remoto, no autenticado, ejecutar código arbitrario y realizar otras acciones no autorizadas en un sistema vulnerable.

Solución:

Aplicar las últimas actualizaciones de su fabricante. Para más información consulte la sección de referencias.

Detalle:

Las vulnerabilidades presentes en el software de los dispositivos codificadores de vídeo PTV/H.264/H.265 son del tipo:

- Acceso administrativo completo mediante una contraseña de puerta trasera. Se ha reservado el identificador CVE-2020-24215 para esta vulnerabilidad.
- Acceso administrativo de root mediante una contraseña de puerta trasera. Se ha reservado el identificador CVE-2020-24218 para esta vulnerabilidad.
- Archivo arbitrario leído a través de path transversal. Se ha reservado el identificador CVE-2020-24219 para esta vulnerabilidad.
- Subida de archivos no autenticados. Se ha reservado el identificador CVE-2020-24217 para esta vulnerabilidad.
- Ejecución arbitraria de código mediante la carga de firmware malicioso. Se ha reservado el identificador CVE-2020-24217 para esta vulnerabilidad.
- Ejecución de código arbitrario mediante inyección de comandos. Se ha reservado el identificador CVE-2020-24217 para esta vulnerabilidad.
- Denegación de servicio por desbordamiento de búfer. Se ha reservado el identificador CVE-2020-24214 para esta vulnerabilidad.
- Acceso no autorizado a la transmisión de vídeo a través de RTSP. Se ha reservado el identificador CVE-2020-24216 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, IoT, Vulnerabilidad

---

Vulnerabilidad en WebAccess Node de Advantech

Fecha de publicación: 18/09/2020

Importancia: Alta

Recursos afectados:

WebAccess Node, todas las versiones anteriores a la 9.0.1.

Descripción:

Se ha publicado una vulnerabilidad de severidad alta en WebAccess Node de Advantech que podría permitir a un atacante la escalada de privilegios.

Solución:

Actualizar a la versión 9.0.1.

Detalle:

El producto afectado no cuenta con los permisos adecuados para los recursos utilizados por servicios específicos lo que podría permitir la ejecución de código. Se ha reservado el identificador CVE-2020-16202 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en CodeMeter de Wibu Systems

Fecha de publicación: 18/09/2020

Importancia: Crítica

Recursos afectados:

Las siguientes versiones de CodeMeter Runtime, un administrador de licencias, se ven afectadas:

- todas las versiones anteriores a 7.10a están afectadas por CVE-2020-14509, CVE-2020-14517 y CVE-2020-14519;
- todas las versiones anteriores a 7.10 están afectadas por CVE-2020-16233;
- todas las versiones anteriores a 6.81 están afectadas por CVE-2020-14513;
- todas las versiones anteriores a 6.90 están afectadas por CVE-2020-14515 cuando se utilizan archivos de actualización CmActLicense con CmActLicense Firm Code.

Descripción:

Los investigadores, Sharon Brizinov y Tal Keren, de Claroty, han reportado 6 vulnerabilidades, 2 con severidad crítica y 4 altas, de tipo acceso al búfer con valor de longitud incorrecto, fortaleza de cifrado inadecuada, error de validación de origen, validación incorrecta de datos de entrada, verificación incorrecta de firma criptográfica y liberación de recursos inapropiados.

Solución:

Wibu Systems recomienda tomar las siguientes medidas:

- actualizar a la última versión CodeMeter Runtime,
- ejecutar CodeMeter Runtime solo como cliente,
- utilizar la nueva API REST en lugar de la API interna de WebSockets,
- deshabilitar la API de WebSockets,
- aplicar AxProtector.

Para información más detallada de los avisos que han publicado los distintos fabricantes afectados por estas vulnerabilidades, consultar la sección *5. MITIGATIONS* del aviso de CISA.

Detalle:

- Existen múltiples vulnerabilidades de memoria corrupta, donde el mecanismo del analizador de paquetes no verifica los campos de longitud. Un atacante podría enviar paquetes, especialmente diseñados, para aprovechar estas vulnerabilidades. Se ha asignado el identificador CVE-2020-14509 para esta vulnerabilidad.
- El cifrado del protocolo se puede vulnerar fácilmente y el servidor acepta conexiones externas, lo que podría permitir que un atacante se comunique de forma remota con la API de CodeMeter. Se ha asignado el identificador CVE-2020-14517 para esta vulnerabilidad.
- Esta vulnerabilidad podría permitir que un atacante utilizara la API interna de WebSockets, a través de un *payload* de Java Script específicamente diseñado, que permitiría la alteración o creación de archivos de licencia, al combinarse con la vulnerabilidad CVE-2020-14515. Se ha asignado el identificador CVE-2020-14519 para esta vulnerabilidad.
- CodeMeter y el *software* que lo usa podrían procesar erróneamente un archivo de licencia, específicamente diseñado, debido a campos de longitud no verificados. Se ha asignado el identificador CVE-2020-14513 para esta vulnerabilidad.
- Existe un problema en el mecanismo de verificación de la firma del archivo de licencia, que podría permitir a los atacantes crear archivos de licencia arbitrarios. Se ha asignado el identificador CVE-2020-14515 para esta vulnerabilidad.
- Un atacante podría enviar un paquete, especialmente diseñado, que podría causar que el servidor devuelva paquetes que contengan datos del montículo (*heap*). Se ha asignado el identificador CVE-2020-16233 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Siemens, Vulnerabilidad

---

Múltiples vulnerabilidades en Philips Clinical Collaboration Platform

Fecha de publicación: 18/09/2020

Importancia: Media

Recursos afectados:

Clinical Collaboration Platform versión 12.2.1 y anteriores.

Descripción:

Investigadores del Northridge Hospital Medical Center han reportado varias vulnerabilidades en Clinical Collaboration Platform que podrían permitir a un atacante causar una denegación de servicio (DoS), engañar a un usuario y ejecutar un ataque Cross-site Request Forgery (CSRF) o proporcionar información para otros ataques posteriores.

Solución:

Actualizar Clinical Collaboration Platform a la versión 12.2.5 para solucionar varias vulnerabilidades y el parche 12.2.1.5 para el resto de vulnerabilidades. La vulnerabilidad CVE-2020-16200 requiere la intervención manual para solucionarse.

Los usuarios de Clinical Collaboration Platform pueden contactar con el servicio de soporte regional, o llamar al 1-877-328-2808.

Detalle:

Las vulnerabilidades más importantes reportadas en Clinical Collaboration Platform se refieren a la exposición de un recurso con un control incorrecto proporcionando información a un atacante para un acceso inadecuado al recurso. Para esta vulnerabilidad se ha reservado el identificador CVE-2020-16247.

La otra vulnerabilidad más importante se refiere a una falta de control en la asignación de un recurso limitado, lo que puede utilizarse por un atacante para alterar los recursos consumidos y potencialmente causar una denegación de servicio. Para esta vulnerabilidad se ha reservado el identificador CVE-2020-16200.

Para otras vulnerabilidades detectadas se han reservado los identificadores CVE-2020-16198, CVE-2020-14525 y CVE-2020-14506.

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

---

Múltiples vulnerabilidades en productos MB connect line

Fecha de publicación: 21/09/2020

Importancia: Crítica

Recursos afectados:

- mymbCONNECT24, versión v2.6.1 y anteriores;
- mbCONNECT24, versión v2.6.1 y anteriores.

Descripción:

 ha coordinado las vulnerabilidades reportadas por OTORIO a MB connect line que podrían permitir a un

atacante la divulgación de información.

Solución:

Actualizar los productos afectados a una versión superior a la v2.6.1.

Detalle:

- Una vulnerabilidad de Inyección SQL ciega en *knximport* y en *lancompenent* que podría permitir a un atacante autenticado descubrir información arbitraria. Se han asignado los identificadores CVE-2020-24569 y CVE-2020-24568 para estas vulnerabilidades.
- La vulnerabilidad de tipo *Server-Side Request Forgery* (SSRF) y *Cross-Site Request Forgery* (CSRF) podría permitir a un atacante robar la información de sesión por medio de enlaces especialmente diseñados. Se ha asignado el identificador CVE-2020-24570 para esta vulnerabilidad.
- El uso de un *software* de terceros, obsoleto y sin usar, podría permitir la ejecución remota de código a través de una cadena de explotación.

Etiquetas: Actualización, Virtualización, Vulnerabilidad

Múltiples vulnerabilidades en varios productos de General Electric

Fecha de publicación: 23/09/2020

Importancia: Alta

Recursos afectados:

- GE Digital APM Classic, versiones 4.4 y anteriores;
- GE Reason S20 Ethernet Switch, versiones:
  - S2020, todas las versiones de *firmware* anteriores a 07A06;
  - S2024, todas las versiones de *firmware* anteriores a 07A06;

Descripción:

Guido Marilli, investigador de Accenture Security, y la compañía IOActive han reportado a GE 4 vulnerabilidades, 2 con severidad alta y 2 medias, de tipo omisión de autorización mediante clave controlada por el usuario, uso de un *hash* unidireccional sin *salt* y XSS.

Solución:

- Actualizar GE Digital APM Classic a la versión 4.5 o superiores, contactando con un representante de GE Digital;
- actualizar GE Reason S20 Ethernet Switch a la versión de *firmware* 07A06 o superiores.

Detalle:

- Una vulnerabilidad IDOR (*Insecure Direct Object Reference*) podría permitir que un atacante descargase datos confidenciales relacionados con cuentas de usuario sin tener los privilegios adecuados. Se ha asignado el identificador CVE-2020-16240 para esta vulnerabilidad.
- *Salt* (datos aleatorios utilizados como entrada adicional a una función unidireccional que utiliza el *hash* de datos, una contraseña o una frase de contraseña) no se utiliza para el cálculo *hash* de contraseñas, lo que podría permitir descifrarlas, poniendo a toda la plataforma en riesgo, ya que un usuario autenticado podría recuperar todos los datos de la cuenta de usuario y luego obtener las contraseñas reales. Se ha asignado el identificador CVE-2020-16244 para esta vulnerabilidad.
- El producto afectado es vulnerable a XSS (*Cross-Site Scripting*), que podría permitir que un atacante engañase a los usuarios para que realizasen acciones críticas que incluyen, entre otras, agregar y actualizar cuentas. Se ha asignado el identificador CVE-2020-16242 para esta vulnerabilidad.
- El producto afectado es vulnerable a XSS, que podría permitir a los atacantes engañar a los usuarios para que sigan un enlace o naveguen a una página con código JavaScript malicioso, lo que haría que dicho código sea procesado y ejecutado por la víctima. Se ha asignado el identificador CVE-2020-16246 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad de secuestro de DLL en Eaton 9000x

Fecha de publicación: 28/09/2020

Importancia: Alta

Recursos afectados:

Software de programación y configuración 9000x de Eaton, versión 2.0.38 y anteriores.

Descripción:

El investigador, Yongjun liu, ha reportado una vulnerabilidad, con severidad alta, de tipo secuestro de DLL (*DLL hijacking*).

Solución:

Actualizar el producto afectado a la versión 2.0.41.

Detalle:

Un atacante podría ejecutar código arbitrario reemplazando *vci11un6.DLL* y *cinpl.DLL* cuando la aplicación intenta cargar las DLL para realizar operaciones normales. Se ha asignado el identificador CVE-2020-6654 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en varios productos de B&R Industrial Automation

Fecha de publicación: 30/09/2020

Importancia: Alta

Recursos afectados:

- SiteManager, todas las versiones anteriores a 9.2.620236042;
- GateManager 4260 y 9250, todas las versiones anteriores a 9.0.20262;
- GateManager 8250, todas las versiones anteriores a 9.2.620236042.

Descripción:

Nikolay Sokolik y Hay Mizrachi han reportado 6 vulnerabilidades, 2 con severidad alta y 4 medias, de tipo limitación inadecuada de una ruta de acceso a un directorio restringido (*path transversal*), consumo de recursos descontrolado, exposición de información y autenticación inadecuada.

Solución:

B&R Industrial Automation informa que las vulnerabilidades se han solucionado en las siguientes versiones:

- SiteManager: 9.2.620236042;
- GateManager 4260 y 9250: 9.0.20262;
- GateManager 8250: 9.2.620236042.

Detalle:

- Un atacante autenticado podría leer la configuración del servicio y otra información confidencial, utilizándola para actividades maliciosas en instancias de SiteManager. Se ha asignado el identificador CVE-2020-11641 para esta vulnerabilidad.
- Un atacante autenticado podría desencadenar un reinicio constante de instancias de SiteManager, lo que limitaría su disponibilidad. Se ha asignado el identificador CVE-2020-11642 para esta vulnerabilidad.
- Un atacante autenticado podría recopilar información sobre dispositivos que pertenecen a una organización extranjera y hacer uso de esta información para actividades maliciosas. Se ha asignado el identificador CVE-2020-11643 para esta vulnerabilidad.
- Un atacante autenticado podría engañar a los usuarios de dominios extranjeros con mensajes o alertas de auditoría falsos. Se ha asignado el identificador CVE-2020-11644 para esta vulnerabilidad.
- Un atacante autenticado podría activar repetidamente un reinicio de las instancias de GateManager, lo que limitaría su disponibilidad. Se ha asignado el identificador CVE-2020-11645 para esta vulnerabilidad.
- Un atacante autenticado podría obtener información sobre todos los dispositivos que pertenecen a su dominio y usar esa información para actividades maliciosas. Se ha asignado el identificador CVE-2020-11646 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad