Boletín de agosto de 2019

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en Arena Simulation Software de Rockwell Automation

Fecha de publicación: 02/08/2019

Importancia: Alta

Recursos afectados:

Arena Simulation Software para Manufacturing, Cat. 9502-Ax, versiones 16.00.00 y anteriores.

Descripción:

El investigador kimiya, de 9SG Security Team, conjuntamente con Zero Day Initiative (ZDI), han reportado varias vulnerabilidades de tipo uso de memoria después de ser liberada y exposición de información, que afectan al producto Arena Simulation Software de Rockwell Automation. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante provocar un fallo en la sesión, dando lugar a una condición de denegación de servicio (DoS) o a la ejecución de código arbitrario.

Solución:

Rockwell Automation ha publicado la versión 16.00.01 de Arena Simulation Software para solucionar estas vulnerabilidades.

Detalle:

- Un fichero Arena especialmente diseñado, abierto por un usuario, podría provocar un fallo en la aplicación o la ejecución de código arbitrario. Se ha reservado el identificador CVE-2019-13510 para esta vulnerabilidad.
- Un fichero Arena especialmente diseñado, abierto por un usuario, podría provocar la exposición de información limitada relacionada con la estación de trabajo víctima del ataque. Se ha reservado el identificador CVE-2019-13511 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Escritura fuera de límites en WebAccess HMI Designer de Advantech

Fecha de publicación: 02/08/2019

Importancia: Alta

Recursos afectados:

Advantech WebAccess HMI Designer versión 2.1.9.23 y anteriores.

Descripción:

Mat Powell, de Zero Day Initiative (ZDI), ha reportado una vulnerabilidad de tipo escritura fuera de límites que afecta al software WebAccess HMI Designer de Advantech. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código arbitrario.

Solución:

Advantech ha publicado la versión 2.1.9.31 de WebAccess HMI Designer, que soluciona esta vulnerabilidad.

Detalle:

Debido a una validación inadecuada de los datos proporcionados por el usuario a la hora de procesar archivos MCR especialmente diseñados, el sistema podría escribir fuera del área de búfer prevista, permitiendo la ejecución remota de código. Se ha asignado el identificador CVE-2019-10961 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Lectura fuera de límites en FRENIC Loader de Fuji Electric

Fecha de publicación: 02/08/2019

Importancia: Baja

Recursos afectados:

FRENIC Loader versión 3.5.0.0 y anteriores.

Descripción:

Kimiya de 9SG Security Team, en colaboración con Zero Day Initiative (ZDI), ha reportado una vulnerabilidad de tipo lectura fura de límites que afecta a FRENIC Loader de Fuji Electric. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante la divulgación de información.

Solución:

Fuji Electric ha publicado una nueva versión de FRENIC Loader que soluciona esta vulnerabilidad.

Detalle:

El producto afectado es vulnerable a una lectura fuera de límites, lo que podría permitir a un atacante la lectura de información limitada del dispositivo. Se ha asignado el identificador CVE-2019-13512 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos EZAutomation

Fecha de publicación: 13/08/2019

Importancia: Alta

Recursos afectados:

- EZTouch Editor.
- EZPLC.

Descripción:

El equipo de 9sg Security Team ha reportado dos vulnerabilidades de tipo desbordamiento de búfer y corrupción de memoria en análisis de archivos, que podrían permitir a un atacante remoto la ejecución de código arbitrario en instalaciones vulnerables de EZTouch Editor y EZPLC.

Solución:

Dada la naturaleza de la vulnerabilidad, la única estrategia de mitigación es restringir la interacción con la aplicación.

Detalle:

- La validación incorrecta de los datos proporcionados por el usuario en archivos EZC origina un estado de memoria corrupta que podría permitir a un atacante remoto la ejecución de código en el contexto del proceso actual en instalaciones del producto EZPLC. Es necesaria la interacción de otro usuario, para que acceda a una página maliciosa o abra un archivo malicioso.
- La validación incorrecta del tamaño de los datos proporcionados por el usuario antes de copiarlos en el búfer, en archivos EZP, podría permitir a un atacante remoto la ejecución de código en el contexto del proceso actual en instalaciones del producto EZTouch Editor. Es necesaria la interacción de otro usuario, para que acceda a una página maliciosa o abra un archivo malicioso.

Etiquetas: 0day, Vulnerabilidad

Múltiples vulnerabilidades en productos Siemens

Fecha de publicación: 13/08/2019

Importancia: Alta

Recursos afectados:

- SCALANCE X-200, todas las versiones.
- SCALANCE X-200IRT, todas las versiones.
- SCALANCE X-200RNA, todas las versiones.
- SIMATIC ET 200SP Open Controller CPU 1515SP PC, todas las versiones.
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2, todas las versiones.

- SIMATIC S7-1200 familia CPU, todas las versiones.
- SIMATIC S7-1500 familia CPU, todas las versiones superiores a la V4.0.
- SIMATIC S7-1500 Software Controller, todas las versiones.
- SIMATIC S7-PLCSIM Advanced, todas las versiones.
- SINAMICS GH150 V4.7 (Control Unit), todas las versiones.
- SINAMICS GH150 V4.8 (Control Unit), todas las versiones inferiores a la V4.8 SP2 HF6.
- SINAMICS GL150 V4.7 (Control Unit), todas las versiones.
- SINAMICS GL150 V4.8 (Control Unit), todas las versiones inferiores a la V4.8 SP2 HF7.
- SINAMICS GM150 V4.7 (Control Unit), todas las versiones.
- SINAMICS GM150 V4.8 (Control Unit), todas las versiones inferiores a la V4.8 SP2 HF9.
- SINAMICS SL150 V4.7 (Control Unit), todas las versiones.
- SINAMICS SL150 V4.8 (Control Unit), todas las versiones.
- SINAMICS SM120 V4.7 (Control Unit), todas las versiones.
- SINAMICS SM120 V4.8 (Control Unit), todas las versiones.
- SCALANCE SC-600, versión V2.0.
- SCALANCE XB-200, versión V4.1.
- SCALANCE XC-200, versión V4.1.
- SCALANCE XF-200BA, versión V4.1.
- SCALANCE XP-200, versión V4.1.
- SCALANCE XR-300WG, versión V4.1.

Descripción:

Diversos investigadores han reportado varias vulnerabilidades que, de ser explotadas, permitirían realizar ataques de denegación de servicio *man-in-the-middle* (MitM), modificación del código fuente del programa y ejecución de comandos arbitrarios.

Solución:

Siemens ha desarrollado diferentes actualizaciones para los dispositivos afectados.

Detalle:

- El dispositivo contiene una vulnerabilidad que permitiría a un atacante crear una condición de denegación de servicio, enviando grandes paquetes de mensajes repetidamente al servicio Telnet. Se ha reservado el identificador CVE-2019-10942 para esta vulnerabilidad.
- El servidor web de los dispositivos afectados contiene una vulnerabilidad que puede ser aprovechada por un atacante para generar una condición de denegación de servicio y lograr el reinicio del servidor web del dispositivo afectado. Se ha asignado el identificador CVE-2019-6568 para esta vulnerabilidad.

Para el resto de las vulnerabilidades, de severidad media y baja, se han reservado los identificadores CVE-2019-10929, CVE-2019-10943, CVE-2019-10927 y CVE-2019-10928.

Etiquetas: Actualización, Comunicaciones, Siemens, Vulnerabilidad

---

Múltiples vulnerabilidades en OSIsoft PI Web API

Fecha de publicación: 14/08/2019

Importancia: Alta

Recursos afectados:

OSIsoft PI Web API, versión 2018 y anteriores.

Descripción:

OSIsoft ha detectado dos vulnerabilidades de inclusión de información sensible en archivos de *log* y de fallo de mecanismo de protección contra ataques CSRF.

Solución:

OSIsoft recomienda a los usuarios actualizar a la versión PI Web API 2018 SP1 o posterior para corregir estas vulnerabilidades.

Detalle:

- Los ficheros de *log* creados por la aplicación OSIsoft PI Web, ante ciertos eventos, exponen información sensible, que puede ser aprovechada por un atacante para realizar ataques más sofisticados. Se ha reservado el identificador CVE-2019-13515 para esta vulnerabilidad.
- Los mecanismos de protección contra ataques de tipo CSRF (*Cross-Site Request Forgery*) implementados en la aplicación no son efectivos en la versión vulnerable. Se ha reservado el identificador CVE-2019-13516 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Delta Industrial Automation DOPSoft

Fecha de publicación: 14/08/2019

Importancia: Alta

Recursos afectados:

- DOPSoft Version 4.00.06.15 y anteriores.

Descripción:

El investigador Kimiya, de 9SG Security Team, ha reportado varias vulnerabilidades de tipo lectura fuera de límites y uso de posiciones de memoria previamente liberada que podrían permitir la filtración de información, la ejecución remota de código o provocar el fallo de la aplicación.

Solución:

Delta Electronics recomienda a los usuarios afectados la actualización a la versión 4.00.06.47 o posterior, así como restringir la interacción con la aplicación a archivos confiables.

Detalle:

- El procesado de un archivo de proyecto, especialmente diseñado, podría causar una vulnerabilidad de tipo uso de memoria previamente liberada o múltiples vulnerabilidades de lectura fuera de límites, lo que podría permitir la filtración de información, la ejecución de código remoto o el fallo de la aplicación. Se han asignado los códigos CVE-2019-13514 y CVE-2019-13513 para estas vulnerabilidades.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Schneider Electric

Fecha de publicación: 14/08/2019

Importancia: Crítica

Recursos afectados:

- Magelis HMIGTO series, todas las versiones.
- Magelis HMISTO series, todas las versiones.
- Magelis XBTGH series, todas las versiones.
- Magelis HMIGTU series, todas las versiones.
- Magelis HMIGTUX series, todas las versiones.
- Magelis HMISCU series, todas las versiones.
- Magelis HMISTU series, todas las versiones.
- Magelis XBTGT series, todas las versiones.
- Magelis XBTGC series, todas las versiones.
- Magelis HMIGXO series, todas las versiones.
- Magelis HMIGXU series, todas las versiones.
- Controlador Modicon M340, todas las versiones.
- Módulo BMXNOR0200H Ethernet / Serial RTU, todas las versiones.
- SoMachine HVAC, versión 2.4.1 y anteriores.
- TelevisGo fabricados antes del 15/07/2019.
- Componente Schneider Electric Software Update (SESU) - SUT Service, desde la versión 2.1.1 hasta la 2.3.0.
- spaceLYnk, todas las versiones anteriores a la 2.4.0.
- Wiser para KNX (homeLYnk), todas las versiones anteriores a la 2.4.0.

Descripción:

Diversos investigadores han reportado varias vulnerabilidades de gestión inadecuada de condiciones excepcionales, control de acceso inapropiado, control sobre el directorio de búsqueda de recursos, restricción inadecuada del búfer de memoria, gestión inadecuada de recursos, lectura y escritura fuera de límites, gestión incorrecta del búfer de memoria, errores de gestión de recursos, interpretación incorrecta de datos y autenticación incorrecta. La explotación de estas vulnerabilidades permitiría a un atacante bloquear el HMI, generar una condición de denegación de servicio, desconectar las conexiones activas, ejecución de comandos por un usuario no autorizado, ejecución de código arbitrario en el dispositivo, ejecución remota de código, provocar desbordamiento de memoria del búfer y la pérdida del control cuando un atacante omite la autenticación.

Solución:

- EcoStruxure Machine Expert HVAC, version 1.1.0.
- TelevisGo, versiones posteriores al 15/07/2019. Para las versiones anteriores, instalar TelevisGo_HotFix_20190715.exe.
- SESU - SUT Service, versión 2.3.1.
- spaceLYnk, versiones de *firmware* 2.4.0_HW_1_X_X y 2.4.0_HW_2_X_X_HW_3_X_X.
- Wiser para KNX, versiones de *firmware* 2.4.0_HW_1_X_X y 2.4.0_HW_2_X_X_HW_3_X_X.
- Para el resto de productos sin actualización concreta, aplicar las medidas de mitigación y buenas prácticas.

Detalle:

A continuación, se detallan las vulnerabilidades de severidad crítica:

- Una restricción incorrecta de las operaciones en el búfer de memoria en el producto UltraVNC, integrado en TelevisGO, permitiría a un atacante con acceso a la red donde se encuentra el sistema afectado, ejecutar código remoto. Se han asignado los identificadores CVE-2019-8258 y CVE-2018-15361 para esta vulnerabilidad.
- Una lectura fuera de límites del búfer de memoria en el producto UltraVNC, integrado en TelevisGO, permitiría a un atacante con acceso a la red donde se encuentra el sistema afectado, obtener información sensible. Se han asignado los identificadores CVE-2019-8260 y CVE-2019-8261 para esta vulnerabilidad.
- Una serie de errores en el búfer de memoria del producto UltraVNC, integrado en TelevisGO, permitirían a un atacante con acceso a la red donde se encuentra el sistema afectado, ejecutar código remoto. Se han asignado los identificadores CVE-2019-8262, CVE-2019-8273, CVE-2019-8274 y CVE-2019-8271 para esta vulnerabilidad.
- La lectura y escritura fuera de límites del búfer de memoria en el producto UltraVNC, integrado en TelevisGO, permitiría a un atacante con acceso a la red donde se encuentra el sistema afectado, ejecutar código remoto. Se han asignado los identificadores CVE-2019-8280, CVE-2019-8264, CVE-2019-8265 y CVE-2019-8266 para esta vulnerabilidad.
- Una gestión incorrecta del tamaño del búfer originada por los cálculos incorrectos ejecutados en el producto UltraVNC, integrado en TelevisGO, permitiría a un atacante con acceso a la red donde se encuentra el sistema afectado, ejecutar código remoto. Se han asignado los identificadores CVE-2019-8268 y CVE-2019-8272 para esta vulnerabilidad.
- Una gestión incorrecta en el control de accesos del producto UltraVNC, integrado en TelevisGO, permitiría a un potencial atacante con acceso a la red donde se encuentra el sistema afectado, acceder a datos fuera de los límites establecidos para cada usuario. Se ha asignado el identificador CVE-2019-8275 para esta vulnerabilidad.

Para el resto de las vulnerabilidades, de severidad alta y media, se han asignado los identificadores: CVE-2019-8259, CVE-2019-8263, CVE-2019-8267, CVE-2019-8276, CVE-2019-8277, CVE-2019-8269, CVE-2019-8270, CVE-2019-6826, CVE-2019-6813, CVE-2019-6831,

CVE-2019-6810, CVE-2019-6813, CVE-2019-6833, CVE-2019-6834 y CVE-2019-6832.

Etiquetas: Actualización, Comunicaciones, Privacidad, Schneider Electric, Vulnerabilidad

---

Desbordamiento de búfer en Alpha5 Smart Loader de Fuji Electric

Fecha de publicación: 16/08/2019

Importancia: Alta

Recursos afectados:

- Alpha5 Smart Loader, todas las versiones anteriores a la 4.2.

Descripción:

El investigador Natnael Samson, trabajando de manera conjunta con Trend Micro's Zero Day Initiative, ha reportado una vulnerabilidad de tipo desbordamiento de búfer en el software Alpha5 Smart Loader, que podría permitir, a un atacante, la ejecución de código con los mismos privilegios que tenga la aplicación.

Solución:

Actualizar a la versión 4.2

Detalle:

Un atacante podría manipular el fichero del proyecto de manera malintencionada para provocar el desbordamiento de búfer en la aplicación Alpha5 Smart Loader, para ejecutar código bajo los privilegios con los que se esté ejecutando dicha aplicación. Se ha reservado el identificador CVE-2019-13520 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en los sistemas Metasys building automation de Johnson Controls

Fecha de publicación: 16/08/2019

Importancia: Media

Recursos afectados:

- Sistema de automatización Metasys building automation, todas las versiones anteriores a la 9.0

Descripción:

El investigador harpocrates.ghost ha reportado varias vulnerabilidades de tipo reutilización de claves de encriptación y claves embebidas en código, que podrían permitir a un atacante remoto, descifrar las comunicaciones de red, afectando a la confidencialidad de las mismas.

Solución:

El fabricante Johnson Controls, recomienda actualizar a versiones posteriores a la v9.0 y configurar las comunicaciones para utilizar certificados de confianza.

Detalle:

- Los servidores ADS/ADX de Metasys y los motores NAE/NIE/NCE, comparten ciertas claves de cifrado RSA utilizadas para la operación contra el Site Management Portal (SMP). Un atacante con acceso a estas claves compartidas RSA, podría descifrar las comunicaciones, tanto de los servidores ADS/ADX como de los NAE/NIE/NCE, realizadas contra el cliente SMP. Se ha asignado el identificador CVE-2019-7593 para esta vulnerabilidad.
- Los servidores ADS/ADX de Metasys y los motores NAE/NIE/NCE, utilizan claves RC2 embebidas para ciertas operaciones contra el Site Management Portal (SMP). Un atacante con acceso a estas claves embebidas RC2, podría descifrar las comunicaciones realizadas entre los servidores ADS/ADX como de los motores NAE/NIE/NCE, realizadas contra el cliente SMP. Se ha asignado el identificador CVE-2019-7594 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en ProSyst mBS SDK y IoT Gateway Software de Bosch

Fecha de publicación: 20/08/2019

Importancia: Crítica

Recursos afectados:

- ProSyst mBS SDK, versiones anteriores a la 8.2.6;
- Bosch IoT Gateway Software, versiones anteriores a la 9.0.2, 9.2.0 y la 9.3.0.

Descripción:

Se han identificado múltiples vulnerabilidades del tipo salto de ruta, Server-Side Request Forgery (SSRF) y exposición de información en los productos afectados, que podrían permitir, a un atacante remoto, acceder a información sensible, escribir y borrar información del sistema y enviar una petición GET de HTTP en nombre del servidor.

Solución:

Actualizar ProSyst mBS SDK a la versión 8.2.6 e IoT Gateway a la versión 9.3.0.

Detalle:

- Una vulnerabilidad de tipo salto de ruta en el acceso remoto a la función *Backup/Restore*, podría permitir a un atacante remoto escribir y borrar ficheros de cualquier localización. Se ha asignado el identificador CVE-2019-11601 para esta vulnerabilidad.
- Una vulnerabilidad del tipo Server-Side Request Forgery (SSRF) en la función *Backup/Restore,* podría permitir a un atacante falsificar peticiones GET a URLs arbitrarias o leer ficheros zip del servidor local. Se ha asignado el identificador CVE-2019-11897 para esta vulnerabilidad.
- La filtración de las trazas de la pila en los accesos remotos de la función *Backup/Restore* podría permitir, a un atacante en remoto, la obtención de información sobre la estructura del sistema. Se ha asignado el identificador CVE-2019-11602 para esta vulnerabilidad.
- Una vulnerabilidad de salto de ruta HTTP podría permitir, a un atacante, la lectura de ficheros fuera de la raíz del servidor web. Se ha asignado el identificador CVE-2019-11603 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Credenciales protegidas inapropiadamente en las impresoras industriales de Zebra

Fecha de publicación: 21/08/2019

Importancia: Media

Recursos afectados:

- Todas las impresoras industriales de Zebra.

Descripción:

El investigador, Tri Quach, ha reportado una vulnerabilidad del tipo credenciales protegidas inapropiadamente en las impresoras industriales de Zebra que podría permitir, a un atacante remoto, el envío de paquetes, especialmente diseñados, a un puerto específico de la impresora para obtener la contraseña del panel de control frontal.

Solución:

Aplicar la actualización Link-OS v6.0.

Detalle:

Al aplicar la opción, desactivada por defecto, de acceso al panel frontal de la impresora mediante código, un atacante podría obtener el código de acceso mediante el envío de paquetes, especialmente diseñados, a un puerto de la impresora, a través de la misma red y utilizarlo para acceder a todas las funcionalidades del panel frontal.

Etiquetas: Actualización, Vulnerabilidad

Desbordamiento de búfer en LeviStudioU de WECON

Fecha de publicación: 22/08/2019

Importancia: Alta

Recursos afectados:

- LeviStudioU.

Descripción:

El investigador Mat Powell, de Zero Day Initiative, ha reportado una vulnerabilidad del tipo desbordamiento de búfer que afecta a LeviStudioU de WECON y que podría permitir a un atacante remoto ejecutar código con privilegios de administrador.

Solución:

Se recomienda restringir la interacción con el servicio a únicamente máquinas de confianza.

Detalle:

Al analizar el elemento ShortMessage SMtext, el proceso no valida correctamente la longitud de los datos proporcionados por el usuario antes de copiarlos en un búfer de longitud fija. Un atacante podría aprovecharse de esta vulnerabilidad para ejecutar código con privilegios de administrador.

Etiquetas: 0day, Vulnerabilidad

Desbordamiento de búfer en enteliBUS Controllers de Delta Controls

Fecha de publicación: 28/08/2019

Importancia: Crítica

Recursos afectados:

- enteliBUS Manager versiones de firmware 3.40 R5 build 571848 y anteriores;
- enteliBUS Manager Touch (eBMGR-TCH) versiones de firmware 3.40 R5 build 571848 y anteriores;
- enteliBUS Controller (eBCON) versiones de firmware 3.40 R5 build 571848 y anteriores.

Descripción:

Los investigadores, Douglas McKee y Mark Bereza, de McAfee Advanced Threat Research, han reportado una vulnerabilidad del tipo desbordamiento de búfer que afecta a equipamiento enteliBUS Controllers de Delta Controls. Un atacante, en la misma red, podría conseguir acceso completo al dispositivo y ejecutar código con privilegios de administrador.

Solución:

Delta Controls ha publicado la actualización enteliBUS 3.40 R6 build 612850. Este nuevo firmware es únicamente accesible para partners registrados. Para poder obtener la actualización se recomienda contactar con Delta Controls o un distribuidor.

Detalle:

La vulnerabilidad de desbordamiento de búfer se debe a la falta de validación de la entrada. Un atacante remoto podría ejecutar código arbitrario. Se ha asignado el identificador CVE-2019-9569 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Evasión de autenticación en AV7000 Linear Barcode Scanner de Datalogic

Fecha de publicación: 28/08/2019

Importancia: Alta

Recursos afectados:

Todas las versiones de AV7000, anteriores a la 4.6.0.0

Descripción:

Los investigadores, Tri Quach y Blake Johnson, del grupo Customer Fulfillment Technology Security (CFS) de Amazon, han reportado una vulnerabilidad del tipo evasión de autenticación en AV7000 de Datalogic.

Solución:

Datalogic ha reportado la liberación de una nueva versión del firmware que soluciona dicha vulnerabilidad. Los usuarios afectados deberán contactar con Datalogic para obtenerla.

Detalle:

La vulnerabilidad de evasión de autenticación mediante el uso de un canal o ruta alternativa, podría permitir a un atacante ejecutar código arbitrario remoto. Se ha asignado el identificador CVE-2019-13526 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Uso de funciones obsoletas en HDI 4000 Ultrasound Systems de Philips

Fecha de publicación: 30/08/2019

Importancia: Baja

Recursos afectados:

Philips HDI 4000 Ultrasound Systems, todas las versiones que se ejecuten en sistemas operativos antiguos y sin soporte, como Windows 2000.

Descripción:

Check Point ha reportado una vulnerabilidad del tipo uso de funciones obsoletas que afecta a equipamiento HDI 4000 Ultrasound System de Philips y que podría permitir la filtración de imágenes de ultrasonidos y el compromiso de la integridad de estas.

Solución:

El ciclo de soporte de este producto terminó el 31 de diciembre de 2013, por lo que no se debería esperar un soporte o actualización por parte de Philips. Los usuarios deberían implementar controles para limitar el acceso a la red y considerar el reemplazar el producto por uno más moderno, con un sistema operativo con soporte.

Detalle:

HDI 4000 Ultrasound System está integrado en un sistema operativo antiguo y sin soporte, cualquier vulnerabilidad existente en dicho sistema operativo podría afectar al producto. Se ha asignado el identificador CVE-2019-10988 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Permisos por defecto incorrectos en equipos de Change Healthcare

Fecha de publicación: 30/08/2019

Importancia: Alta

Recursos afectados:

- Horizon Cardiology, versiones 12.x y anteriores;
- McKesson Cardiology, versiones pertenecientes a las ramas 14.x y 13.x;
- Change Healthcare Cardiology, versiones perteneciente a la rama 14.1.x.

Descripción:

Los investigadores, Alfonso Powers y Bradley Shubin, del grupo Asante Information Security, han reportado una vulnerabilidad de criticidad alta que afecta al equipamiento de Change Healthcare. Un atacante local, autenticado, podría realizar ejecución de código arbitrario.

Solución:

Change Healthcare recomienda a los usuarios afectados contactar con su departamento de soporte lo antes posible para concertar la instalación del parche.

Detalle:

La vulnerabilidad se debe a permisos inseguros en algunos archivos en la instalación por defecto del sistema. Un atacante, con acceso local al sistema, podría ejecutar código arbitrario. Se ha reservado el identificador CVE-2018-18630 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad