Boletín de noviembre de 2019

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en productos de Moxa

Fecha de publicación: 20/11/2019

Importancia: Crítica

Recursos afectados:

- EDS-G508E Series, versión 6.0 y anteriores,
- EDS-G512E Series, versión 6.0 y anteriores,
- EDS-G516E Series, versión 6.0 y anteriores,
- EDR-810 Series, versión 5.1 y anteriores.

Descripción:

Los investigadores Yuval Ardon y Matan Dobrushin, de Otorio, junto con Neil Pope y Rhys Cable, de Motherwell Avanced Technologies Cyber Review Team, han reportado vulnerabilidades con severidades críticas en productos de Moxa. Un atacante remoto podría dejar el dispositivo fuera de servicio, generar una condición de denegación de servicio o la ejecución arbitraria de comandos.

Solución:

Moxa ha publicado actualizaciones que mitigan las vulnerabilidades:

- Para los productos EDS-G508E Series, EDS-G512E Series, EDS-G516E Series, contactar con el servicio de soporte técnico de Moxa, para obtener la actualización.
- Para el dispositivo EDR-810 Series está disponible la descarga del nuevo firmware.

Detalle:

- La vulnerabilidad reside en los paquetes de descubrimiento de dispositivos PROFINET DCE-RPC. Un atacante remoto podría inutilizar o generar una condición de denegación de servicio en el dispositivo.
- La falta de saneamiento en elementos especiales empleados en la interfaz de usuario web (*Web GUI*) podría permitir a un atacante remoto, mediante una petición HTTP POST, específicamente creada, realizar una ejecución arbitraria de comandos. Se ha reservado el identificador CVE-2019-14374 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Siemens

Fecha de publicación: 12/11/2019

Importancia: Alta

Recursos afectados:

- Nucleus NET: todas las versiones;
- Nucleus RTOS: todas las versiones;
- Nucleus ReadyStart para ARM, MIPS y PPC: todas las versiones anteriores a 2017.02.2;
- Nucleus SafetyCert: todas las versiones;
- Nucleus Source Code: todas las versiones;
- VSTAR: todas las versiones;
- CPU S7-1200: todas las versiones;
- controladores de automatización Designo PX, todas las versiones de *firmware* anteriores a 6.00.320, de los siguientes productos:
  - PXC00-E.D, PXC50-E.D, PXC100-E.D, PXC200-E.D con los módulos Desigo PX Web PXA40-W0, PXA40-W y PXA40-W2;
  - PXC00-U, PXC64-U y PXC128-U con los módulos Desigo PX Web PXA30-W0, PXA30-W1 y PXA30-W2;

- PXC22.1-E.D, PXC36-E.D y PXC36.1-E.D con el servidor web activado.

Descripción:

Se han publicado múltiples vulnerabilidades que afectan a dispositivos de Siemens. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto, no autenticado, dañar la integridad y disponibilidad del dispositivo, causar una condición de denegación de servicio y acceder a funciones adicionales de diagnóstico.

Solución:

- Nucleus ReadyStart para ARM, MIPS y PPC: actualizar a la versión 2017.02.2 e instalar el parche *Nucleus 2017.02.02 Nucleus NET Patch*;
- Nucleus SafetyCert: este producto no está afectado directamente, sin embargo, su *bundle* contiene una copia de Nucleus ReadyStart, que sí está afectado, y cuya solución se muestra en el anterior *bullet;*
- controladores de automatización Designo PX: instalar la versión 6.00.320 o posterior;
- Para el resto de productos afectados, consultar las recomendaciones de la sección *Workarounds and Mitigations* de los avisos oficiales de Siemens.

Detalle:

- Un atacante podría comprometer la integridad y la disponibilidad de un dispositivo mediante el envío de paquetes DHCP especialmente diseñados. Se ha reservado el identificador CVE-2019-13939 para esta vulnerabilidad.
- Un atacante con acceso físico a la interfaz UART durante el proceso de arranque, podría acceder a funciones adicionales de diagnóstico. Se ha reservado el identificador CVE-2019-13945 para esta vulnerabilidad.
- Un atacante podría provocar una condición de denegación de servicio en el servidor web del dispositivo, mediante el envío de paquetes HTTP especialmente diseñados al puerto del servidor web (tcp/80). Se ha reservado el identificador CVE-2019-13927 para esta vulnerabilidad.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en productos de Honeywell

Fecha de publicación: 04/11/2019

Importancia: Alta

Recursos afectados:

- equIP Series IP Cameras.
- equIP y Performance Series IP Cameras y Recorders.

Descripción:

El equipo de Honeywell ha publicado múltiples vulnerabilidades, de tipo validación de entrada incorrecta, ausencia de autenticación para funciones críticas y omisión de autenticación.

Solución:

Honeywell ha desarrollado diferentes actualizaciones para los dispositivos afectados.

Detalle:

- Existe una vulnerabilidad en los productos afectados donde una petición de paquete HTTP, especialmente diseñada, podría resultar en una denegación de servicio. Se ha asignado el identificador CVE-2019-18228 para esta vulnerabilidad.
- Un atacante remoto podría acceder al audio del dispositivo a través de una petición HTTP sin ningún tipo de autenticación. Se ha asignado el identificador CVE-2019-18230 para esta vulnerabilidad.
- Existe una vulnerabilidad, de tipo ataque de repetición, al mantenerse un método de autenticación débil para la compatibilidad con los productos heredados. Se ha asignado el identificador CVE-2019-18226 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en WISE-PaaS/RMM de Advantech

Fecha de publicación: 04/11/2019

Importancia: Crítica

Recursos afectados:

WISE-PaaS/RMM versión 3.3.29 y anteriores.

Descripción:

El equipo de rgod de 9sg Security Team y trendytofu han reportado cuatro vulnerabilidades, dos con severidad crítica, una alta y otra media. Un atacante remoto podría provocar la ejecución de código de forma remota con privilegios de administrador, uso de funciones sin autenticación, acceso a información sensible e inyección de comandos SQL.

Solución:

Advantech ha remplazado WISE-PaaS/RMM en julio de 2019 por EdgeSense y DeviceOn y recomiendan substituir el software vulnerable por el nuevo, el cual dispone de soporte.

Detalle:

- Las vulnerabilidades de severidad crítica son:
  - La falta de validación en las rutas de directorios puede permitir a un atacante la ejecución de código remoto mientras se hace pasar por un administrador. Se ha asignado el identificador CVE-2019-13551 para esta vulnerabilidad.
  - Existe una función que permite a cualquiera, que pudiese acceder a la dirección IP, utilizar dicha función sin necesidad de autenticación. Se ha asignado el identificador CVE-2019-13547 para esta vulnerabilidad.
- La vulnerabilidad de criticidad alta es:
  - Existen una serie de vulnerabilidades XXE que podrían permitir a un atacante revelar información sensible. Se ha asignado el identificador CVE-2019-18227 para esta vulnerabilidad.
- La vulnerabilidad de criticidad media es:
  - La falta de tratamiento de las entradas del usuario podrían permitir a un atacante la inyección de comandos SQL, y a través de esta, podría revelar información sensible. Se ha asignado el identificador CVE-2019-18229 para esta vulnerabilidad.

Etiquetas: Vulnerabilidad

Falta de autenticación en varios productos de ABB

Fecha de publicación: 04/11/2019

Importancia: Crítica

Recursos afectados:

- Power Generation Information Manager (PGIM), todas las versiones,
- Plant Connect, todas las versiones.

Descripción:

El investigador Rikard Bodforss de Bodforss Consulting, ha reportado una vulnerabilidad crítica en productos de ABB. Un atacante remoto podría evadir la autenticación, extraer las credenciales, modificar la configuración del PGIM History y los eventos de la base de datos.

Solución:

ABB recomienda emplear el producto actualizado, Symphony Plus Historian, el cual está disponible y resuelve dicha vulnerabilidad.

Detalle:

La insuficiencia de protecciones en las credenciales de usuario y en los mecanismos de autenticación podrían permitir a un atacante remoto obtener las credenciales de usuario de PGIM y posteriormente, alterar la configuración tanto del PGIM como de las bases de datos.

Etiquetas: Vulnerabilidad

Vulnerabilidad de uso de función obsoleta en CX-Supervisor de Omron

Fecha de publicación: 06/11/2019

Importancia: Alta

Recursos afectados:

CX-Supervisor, versión 3.5 (12) y anteriores.

Descripción:

El investigador Michael DePlante, de Micro's Zero Day Initiative, ha reportado una vulnerabilidad de tipo uso de función obsoleta.

Solución:

Actualziar CX-Supervisor a la versión 3.51 (9).

Detalle:

El uso de función obsoleta en el sistema CX-Supervisor podría permitir a un atacante remoto la explotación de dicha vulnerabilidad, pudiendo acceder a información sensible, comprometer todo el sistema y provocar una falta de disponibilidad del equipo. Además, Omron CX-Supervisor se vende con Teamviewer 5.0.8703 QS, una versión que contiene tres vulnerabilidades conocidas. Se han asignado los identificadores CVE-2019-11769, CVE-2018-16550, CVE-2018-14333, y CVE-2010-3128 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en EDS-405A Series de Moxa

Fecha de publicación: 07/11/2019

Importancia: Alta

Recursos afectados:

EDS-405A Series, versión 3.8 y anteriores.

Descripción:

El equipo de Moxa ha reportado vulnerabilidades de tipo denegación de servicio en uno de sus servicios web que podría permitir a un atacante remoto inutilizar el dispositivo, dejando a usuarios autorizados sin la capacidad de acceder al dispositivo.

Solución:

Aplicar el parche de seguridad.

Detalle:

- El envío de un comando HTTP GET, especialmente diseñado, podría permitir a un atacante remoto la denegación del servicio. Esto ocurre debido a que no se comprueba el tamaño del payload del paquete.

Etiquetas: Actualización, Vulnerabilidad

Desbordamiento de búfer en equipamiento V-Server de Fuji Electric

Fecha de publicación: 08/11/2019

Importancia: Alta

Recursos afectados:

V-Server, versión 4.0.6 y anteriores.

Descripción:

Kimiya, de 9SG, junto con Trend Micro's Zero Day Initiative, han detectado una vulnerabilidad de criticidad alta. Un atacante remoto podría realizar un cierre inesperado o la ejecución de código arbitrario en el dispositivo.

Solución:

Fuji Electric ha publicado la versión 4.0.7.0 para solucionar la vulnerabilidad.

Detalle:

La vulnerabilidad se debe a múltiples desbordamientos de búfer basados en pila. Un atacante remoto podría realizar un cierre inesperado o la ejecución de código arbitrario en el dispositivo. Se ha reservado el identificador CVE-2019-18240 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Consumo incontrolado de recursos en múltiples productos de Mitsubishi Electric

Fecha de publicación: 08/11/2019

Importancia: Alta

Recursos afectados:

- MELSEC-Q Series:
  - Q03/04/06/13/26UDVCPU, número de serie 21081 y anteriores;
  - Q04/06/13/26UDPVCPU, número de serie 21081 y anteriores;
  - Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU número de serie 21081 y anteriores.
- MELSEC-L Series:
  - L02/06/26CPU L26CPU-BT, número de serie 21101 y anteriores;
  - L02/06/26CPU-P L26CPU-PBT, número de serie 21101 y anteriores;
  - L02/06/26CPU-CM L26CPU-BT-CM, número de serie 21101 y anteriores.

Descripción:

Tri Quach, de Amazon's Customer Fulfillment Technology Security, ha reportado una vulnerabilidad de tipo consumo incontrolado de recursos. La explotación satisfactoria de esta vulnerabilidad puede impedir que el cliente FTP se conecte al servidor FTP en los productos afectados.

Solución:

Mitsubishi Electric ha liberado una nueva versión del *firmware* para solucionar la vulnerabilidad. Mitsubishi Electric además recomienda a los usuarios que utilicen dicho dispositivo a través de un *firewall*.

Detalle:

Un atacante remoto puede hacer que el servicio FTP introduzca una condición de denegación de servicio, dependiendo del momento en el que en atacante se conecte al servidor FTP en los módulos de CPU afectados. Solamente la función del servidor FTP se ve afectada por esta vulnerabilidad. Se ha reservado el identificador CVE-2019-13555 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidades en productos Valleylab de

Medtronic

Fecha de publicación: 08/11/2019

Importancia: Crítica

Recursos afectados:

- Valleylab LS10 Energy Platform (VLLS10GEN), versión 1.20.2 y anteriores;
- Valleylab Exchange Client, versión 3.4 y anteriores;
- Valleylab FT10 Energy Platform (VLFT10GEN), versión 4.0.0 y anteriores;
- Valleylab FX8 Energy Platform (VLFX8GEN), versión 1.1.0 y anteriores.

Descripción:

El equipo de Medtronic ha reportado múltiples vulnerabilidades de tipo autenticación incorrecta, fallo del mecanismo de protección, uso de credenciales codificadas, uso de algoritmos *hash* reversibles y validación incorrecta de entradas. La explotación de estas vulnerabilidades permitiría a un atacante remoto conectar instrumentos inseguros perdiendo la integridad del sistema, sobrescribir ficheros o ejecutar código de forma remota.

Solución:

Medtronic recomienda actualizar a las nuevas versiones disponibles para solucionar estas vulnerabilidades, contactando con ellos para obtener los nuevos parches.

Detalle:

- El mecanismo de seguridad RFID empleado para la autenticación de los dispositivos FT10/LS10 Energy Platform se puede omitir, permitiendo conectar instrumentos no originales o auténticos al generador. Se ha reservado el identificador CVE-2019-13531 para esta vulnerabilidad.
- El mecanismo de seguridad RFID no aplica protección de lectura, lo que permite un acceso de lectura completo a los datos del mecanismo de seguridad RFID. Se ha reservado el identificador CVE-2019-13535 para esta vulnerabilidad.
- Los productos afectados utilizan varios conjuntos de credenciales codificadas. Si se descubren, se pueden utilizar para leer archivos en el dispositivo. Se ha reservado el identificador CVE-2019-13543 para esta vulnerabilidad.
- Los productos afectados utilizan el algoritmo de descripción para el *hash* de contraseñas del sistema operativo. Mientras que los inicios de sesión interactivos basados en la red están desactivados, los atacantes pueden utilizar las otras vulnerabilidades descritas para obtener acceso local al *shell* y acceder a estos *hashes*. Se ha reservado el identificador CVE-2019-13539 para esta vulnerabilidad.
- Los productos afectados utilizan una versión vulnerable de *rssh* para facilitar la subida de ficheros. Esto permitiría a un atacante con permisos de administrador acceder a ficheros o ejecutar código de forma aleatoria. Se han reservado los identificadores CVE-2019-3464 y CVE-2019-3463 para esta vulnerabilidad.

Etiquetas: Actualización, Sanidad, Vulnerabilidad

Múltiples vulnerabilidades en productos de Siemens

Fecha de publicación: 12/11/2019

Importancia: Alta

Recursos afectados:

- Nucleus NET: todas las versiones;
- Nucleus RTOS: todas las versiones;
- Nucleus ReadyStart para ARM, MIPS y PPC: todas las versiones anteriores a 2017.02.2;
- Nucleus SafetyCert: todas las versiones;
- Nucleus Source Code: todas las versiones;
- VSTAR: todas las versiones;
- CPU S7-1200: todas las versiones;
- controladores de automatización Designo PX, todas las versiones de *firmware* anteriores a 6.00.320, de los siguientes productos:
  - PXC00-E.D, PXC50-E.D, PXC100-E.D, PXC200-E.D con los módulos Desigo PX Web PXA40-W0, PXA40-W y PXA40-W2;
  - PXC00-U, PXC64-U y PXC128-U con los módulos Desigo PX Web PXA30-W0, PXA30-W1 y PXA30-W2;
  - PXC22.1-E.D, PXC36-E.D y PXC36.1-E.D con el servidor web activado.

Descripción:

Se han publicado múltiples vulnerabilidades que afectan a dispositivos de Siemens. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto, no autenticado, dañar la integridad y disponibilidad del dispositivo, causar una condición de denegación de servicio y acceder a funciones adicionales de diagnóstico.

Solución:

- Nucleus ReadyStart para ARM, MIPS y PPC: actualizar a la versión 2017.02.2 e instalar el parche *Nucleus 2017.02.02 Nucleus NET Patch*;
- Nucleus SafetyCert: este producto no está afectado directamente, sin embargo, su *bundle* contiene una copia de Nucleus ReadyStart, que sí está afectado, y cuya solución se muestra en el anterior *bullet;*
- controladores de automatización Designo PX: instalar la versión 6.00.320 o posterior;
- Para el resto de productos afectados, consultar las recomendaciones de la sección *Workarounds and Mitigations* de los avisos oficiales de Siemens.

Detalle:

- Un atacante podría comprometer la integridad y la disponibilidad de un dispositivo mediante el envío de paquetes DHCP especialmente diseñados. Se ha reservado el identificador CVE-2019-13939 para esta vulnerabilidad.
- Un atacante con acceso físico a la interfaz UART durante el proceso de arranque, podría acceder a funciones adicionales de diagnóstico. Se ha reservado el identificador CVE-2019-13945 para esta vulnerabilidad.
- Un atacante podría provocar una condición de denegación de servicio en el servidor web del dispositivo, mediante el envío de

paquetes HTTP especialmente diseñados al puerto del servidor web (tcp/80). Se ha reservado el identificador CVE-2019-13927 para esta vulnerabilidad.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Ejecución arbitraria de código en Automation Builder y Drive Application Builder de ABB

Fecha de publicación: 14/11/2019

Importancia: Alta

Recursos afectados:

- Automation Builder, todas las versiones anteriores a la versión 2.3.0 (solo cuando se utiliza para programar PLC AC500 V3 o las unidades programables IEC61131).
- Drive Application Builder: versión 1.0.0.

Descripción:

El investiagador Heinz FÃ¤glister de WRH Walter Reist Holding AGSe ha identificado una vulnerabilidad de inyección de código que afecta a varios dispositivos de ABB. Un atacante podría realizar una ejecución de código arbitraria.

Solución:

ABB publicará actualizaciones específicas para cada uno de los productos afectados que solucionarán esta vulnerabilidad. Una vez estén disponibles, se recomienda actualizar a dicha versión.

- Automation Builder, actualizar a la versión 2.3.0 disponible en el primer cuatrimestre de 2020.
- Drive Application Builder, actualizar a la versión 1.1.0 disponible a finales de 2019.

Hasta la publicación de las actualizaciones, ABB recomienda utilizar librerías IEC 61131 obtenidas únicamente de fuentes confiables.

Detalle:

La vulnerabilidad se origina en los componentes activos en la documentación de la librería IEC 61131-3. En el entorno de desarrollo se muestran estos componentes activos sin ningún proceso de validación, pudiendo permitir a un atacante la ejecución de código JavaScript o ActiveX.

Etiquetas: Actualización, Vulnerabilidad

Nivel de cifrado inadecuado en IntelliBridge de Philips

Fecha de publicación: 15/11/2019

Importancia: Media

Recursos afectados:

- IntelliBridge EC40 Hub, todas las versiones;
- IntelliBridge EC80 Hub, todas las versiones.

Descripción:

La explotación exitosa de esta vulnerabilidad permitiría el acceso no autorizado de un atacante al *hub* EC40/80 de IntelliBridge, lo que le otorgaría acceso para ejecutar software, modificar la configuración del sistema o ver y actualizar archivos, incluyendo datos de pacientes no identificables.

Solución:

Philips planea publicar una nueva versión para solucionar esta vulnerabilidad a finales del tercer trimestre de 2020.

Detalle:

El servidor SSH que se ejecuta en los productos afectados está configurado para permitir cifrado débil. Esto podría permitir a un atacante, no autorizado, con acceso a la red, capturar y reproducir la sesión y obtener acceso no autorizado al *hub* EC40/80. Se ha reservado el identificador CVE-2019-18241 para esta vulnerabilidad.

Etiquetas: Actualización, Sanidad, Vulnerabilidad

Uso de función obsoleta en CX-Supervisor de Omron

Fecha de publicación: 15/11/2019

Importancia: Alta

Recursos afectados:

CX-Supervisor versión 3.5 (12) y anteriores.

Descripción:

El investigador Michael DePlante, de Trend Micro's Zero Day Initiative, ha reportado una vulnerabilidad de tipo uso de función obsoleta que afecta a CX-Supervisor de Omron. Un atacante remoto podría revelar información o comprometer al sistema y su disponibilidad.

Solución:

Actualizar a la versión CX-Supervisor 3.51(9).

Detalle:

CX-Supervisor de Omron se distribuye con Teamviewer versión 5.0.8703 QS. Esta versión de TeamViewer es vulnerable debido al uso de una función obsoleta que requiere la interacción del usuario para ser explotada. Un atacante remoto podría revelar información o comprometer al sistema y su disponibilidad. Se ha reservado el identificador CVE-2019-18251 para esta vulnerabilidad.

Etiquetas: Actualización, SCADA, Vulnerabilidad

Múltiples vulnerabilidades en productos de Moxa

Fecha de publicación: 20/11/2019

Importancia: Crítica

Recursos afectados:

- EDS-G508E Series, versión 6.0 y anteriores,
- EDS-G512E Series, versión 6.0 y anteriores,
- EDS-G516E Series, versión 6.0 y anteriores,
- EDR-810 Series, versión 5.1 y anteriores.

Descripción:

Los investigadores Yuval Ardon y Matan Dobrushin, de Otorio, junto con Neil Pope y Rhys Cable, de Motherwell Avanced Technologies Cyber Review Team, han reportado vulnerabilidades con severidades críticas en productos de Moxa. Un atacante remoto podría dejar el dispositivo fuera de servicio, generar una condición de denegación de servicio o la ejecución arbitraria de comandos.

Solución:

Moxa ha publicado actualizaciones que mitigan las vulnerabilidades:

- Para los productos EDS-G508E Series, EDS-G512E Series, EDS-G516E Series, contactar con el servicio de soporte técnico de Moxa, para obtener la actualización.
- Para el dispositivo EDR-810 Series está disponible la descarga del nuevo firmware.

Detalle:

- La vulnerabilidad reside en los paquetes de descubrimiento de dispositivos PROFINET DCE-RPC. Un atacante remoto podría inutilizar o generar una condición de denegación de servicio en el dispositivo.
- La falta de saneamiento en elementos especiales empleados en la interfaz de usuario web (*Web GUI*) podría permitir a un atacante remoto, mediante una petición HTTP POST, específicamente creada, realizar una ejecución arbitraria de comandos. Se ha reservado el identificador CVE-2019-14374 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en el servidor web de CODESYS de 3S-Smart Software Solutions GmbH

Fecha de publicación: 20/11/2019

Importancia: Crítica

Recursos afectados:

Todos los sistemas en tiempo de ejecución de CODESYS V3 que contienen el servidor web (*CmpWebServer* y *CmpWebServerHandler*) en todas las versiones anteriores a 3.5.15.20 se ven afectados, 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 PLCnext;
- CODESYS Control para PFC100;
- CODESYS Control para PFC200;
- CODESYS Control para Raspberry Pi;
- CODESYS Control RTE V3;
- CODESYS Control RTE V3 (para Beckhoff CX);
- CODESYS Control Win V3 (también parte de la configuración 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:

Un cliente de OEM y Tenable ha reportado una vulnerabilidad, de tipo desbordamiento de búfer basado en memoria dinámica (*heap*), que afecta a sistemas Codesys V3. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto causar una denegación de servicio o la ejecución de código arbitraria.

Solución:

3S-Smart Software Solutions GmbH ha publicado la versión 3.5.15.20 para solucionar esta vulnerabilidad.

Detalle:

El servidor web de CODESYS es utilizado por CODESYS WebVisu para mostrar las pantallas de visualización de CODESYS en un navegador web. El envío de solicitudes, específicamente diseñadas, puede causar un desbordamiento de búfer basado en memoria dinámica (*heap*). Más adelante, esto podría bloquear el servidor web, provocar una condición de denegación de servicio o puede ser utilizado para la ejecución remota de código. Dado que el servidor web forma parte del sistema de tiempo de ejecución de CODESYS, esto puede dar lugar a un comportamiento imprevisto del sistema de ejecución por completo. Se ha reservado el identificador CVE-2019-18858 para dicha vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en FlexNet Publisher de Flexera

Fecha de publicación: 20/11/2019

Importancia: Crítica

Recursos afectados:

FlexNet Publisher, versión 2018 R3 y anteriores.

Descripción:

El investigador Sergey Temnikov, de Kaspersky, ha reportado vulnerabilidades de tipo validación de entradas incorrecta y corrupción de memoria que afectan a FlexNet Publisher de Flexera. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto negar la adquisición de una licencia válida para el uso legal del producto y la ejecución de código de forma remota.

Solución:

Flexera recomienda actualizar a la versión 2018 R4 o superior.

Detalle:

- Varias vulnerabilidades relacionadas con la eliminación preventiva de elementos, la decodificación de mensajes o la adición de un elemento a una lista en los componentes *lmgrd* y *daemon* del proveedor permite que un atacante remoto envíe una combinación de mensajes a *lmgrd* o a *daemon*, haciendo que el *heartbeat* entre *lmgrd* y *daemon* del proveedor se detenga y que el *daemon* se apague. Se han asignado los identificadores CVE-2018-20031, CVE-2018-20032 y CVE-2018-20034 para estas vulnerabilidades, respectivamente.
- Una vulnerabilidad en los componentes *lmgrd* y *daemon* del proveedor podría permitir que un atacante remoto corrompa la memoria asignando/desasignando memoria, cargando *lmgrd* o *daemon*, y causando que el *heartbeat* entre *lmgrd* y *daemon* se detenga. Esto obligaría al demonio del vendedor a cerrar. Esta vulnerabilidad también podría permitir la ejecución remota de código. Se ha asignado el identificador CVE-2018-20033 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad