Boletín de agosto 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.

Múltiples vulnerabilidades en Industrial Automation CNCSoft ScreenEditor de Delta Electronics

Fecha de publicación: 05/08/2020

Importancia: Alta

Recursos afectados:

Industrial Automation CNCSoft ScreenEditor, versiones 1.01.23 y anteriores.

Descripción:

Se han reportado múltiples vulnerabilidades en Industrial Automation CNCSoft ScreenEditor que podrían permitir a un atacante leer o modificar información, ejecutar código arbitrario o provocar el cierre inesperado del sistema.

Solución:

Actualizar a CNCSoft ScreenEditor versión 1.01.26.

Detalle:

- Múltiples vulnerabilidades del tipo desbordamiento de búfer basado en pila podrían permitir a un atacante leer o modificar información, ejecutar código arbitrario o provocar el cierre inesperado del sistema mediante el procesamiento de archivos de proyecto especialmente diseñados. Se ha asignado el identificador CVE-2020-16199 para esta vulnerabilidad.
- Múltiples vulnerabilidades del tipo lectura fuera de límites podrían permitir a un atacante leer información mediante el procesamiento de archivos de proyecto especialmente diseñados. Se ha asignado el identificador CVE-2020-16201 para esta vulnerabilidad.
- Un puntero no inicializado puede ser explotado mediante el procesamiento de archivos de proyecto especialmente diseñados, lo que podría permitir a un atacante leer o modificar información, ejecutar código arbitrario o provocar el cierre inesperado del sistema. Se ha asignado el identificador CVE-2020-16203 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

Vulnerabilidad de neutralización inadecuada en G-Cam y G-Code de Geutebrück

Fecha de publicación: 07/08/2020

Importancia: Alta

Recursos afectados:

- Versión de *firmware* 1.12.0.25 y anteriores;
- versiones 1.12.13.2 y 1.12.14.5 de los siguientes modelos de Encoder y E2 Series Camera:
  - G-Code:
    - EEC-2xxx,
  - G-Cam:
    - EBC-21xx,
    - EFD-22xx,
    - ETHC-22xx,
    - EWPC-22xx.

Descripción:

Davy Douhine, de RandoriSec, ha reportado al CISA esta vulnerabilidad de severidad alta que podría permitir a un atacante ejecutar comandos como usuario *root*.

Solución:

Actualizar a la versión de *firmware* 1.12.0.27.

Detalle:

La neutralización inadecuada de elementos especiales utilizados en comandos del sistema operativo podría permitir a un atacante ejecutar comandos como usuario *root* mediante un comando URL especialmente diseñado. Se ha reservado el identificador CVE-2020-16205 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en WebAccess HMI Designer de Advantech

Fecha de publicación: 07/08/2020

Importancia: Crítica

Recursos afectados:

WebAccess HMI Designer, versión 2.1.9.31 y anteriores.

Descripción:

Kimiya y Natnael Samson, en colaboración con Zero Day Initiative de Trend Micro, han reportado 6 vulnerabilidades al CISA, una de severidad crítica, 4 altas y una baja, de tipo desbordamiento de búfer basado en pila (*stack*), desbordamiento de búfer basado en montículo (*heap*), lectura fuera de límites, escritura fuera de límites, acceso al recurso mediante un tipo incompatible y doble llamada a la función *free()*.

Solución:

Advantech ha publicado la versión 2.1.9.81 de WebAccess HMI Designer para solucionar estas vulnerabilidades.

Detalle:

- El procesamiento de archivos de proyecto, especialmente diseñados, que carezcan de la validación adecuada de los datos proporcionados por el usuario, podría provocar un desbordamiento del búfer basado en la pila (*stack*), lo que permitiría la ejecución remota de código, la divulgación/modificación de información o causar el bloqueo de la aplicación. Se ha asignado el identificador CVE-2020-16215 para esta vulnerabilidad.
- Se podrían explotar múltiples vulnerabilidades de desbordamiento de búfer basadas en montículo (*heap*) abriendo archivos de proyecto, especialmente diseñados, que permitirían la ejecución remota de código, la divulgación/modificación de información o causar el bloqueo de la aplicación. Se ha asignado el identificador CVE-2020-16207 para esta vulnerabilidad.
- El procesamiento de archivos de proyecto, especialmente diseñados, que carezcan de la validación adecuada de los datos proporcionados por el usuario, podría causar que el sistema escribiera fuera del área de búfer prevista, lo que permitiría la ejecución remota de código, la divulgación/modificación de información o causar el bloqueo de la aplicación. Se ha asignado el identificador CVE-2020-16213 para esta vulnerabilidad.
- El procesamiento de archivos de proyectos, especialmente diseñados, que carecen de la validación adecuada de los datos proporcionados por el usuario, podría causar una condición de confusión de tipos, que permitiría la ejecución remota de código, la divulgación/modificación de información o causar el bloqueo de la aplicación. Se ha asignado el identificador CVE-2020-16229 para esta vulnerabilidad.
- Una vulnerabilidad en la función de liberación de memoria *free()*, causada por el procesamiento de archivos de proyecto especialmente diseñados, podría permitir la ejecución remota de código, la divulgación/modificación de información o causar el bloqueo de la aplicación. Se ha asignado el identificador CVE-2020-16217 para esta vulnerabilidad.
- Una vulnerabilidad de lectura fuera de los límites podría aprovecharse, al procesar archivos de proyecto especialmente diseñados, para permitir que un atacante lea información. Se ha asignado el identificador CVE-2020-16211 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en Delta Industrial Automation TPEditor

Fecha de publicación: 07/08/2020

Importancia: Alta

Recursos afectados:

TPEditor, versiones 1.97 y anteriores.

Descripción:

Se han reportado múltiples vulnerabilidades en el *software* de programación de texto de Delta, TPEditor, que podrían permitir a un atacante leer o modificar información, ejecutar código arbitrario o provocar el cierre inesperado del sistema.

Solución:

Actualizar a Delta Industrial Automation TPEditor, versión 1.98.

Detalle:

Múltiples vulnerabilidades del tipo lectura fuera de límites, desbordamiento de búfer basado en pila, desbordamiento de búfer basado en montículo (*heap*), validación inadecuada de los datos de entrada y una condición de *write-what-where*, podrían permitir a un atacante leer o modificar información, ejecutar código arbitrario o provocar el cierre inesperado del sistema mediante el procesamiento de archivos de proyecto especialmente diseñados. Se han asignado los identificadores CVE-2020-16299, CVE-2020-16221, CVE-2020-16227 y CVE-2020-16225 para estas vulnerabilidades.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Acceso a información sensible en sistemas PLC para remolques

Fecha de publicación: 07/08/2020

Importancia: Media

Recursos afectados:

Todas las comunicaciones a través de la línea eléctrica de los remolques se ven afectadas.

Descripción:

Investigadores de la National Motor Freight Traffic Association (NMFTA) y la Assured Information Security (AIS) han descubierto una vulnerabilidad, de tipo divulgación de información sensible, en sistemas PLC utilizados en remolques de múltiples fabricantes.

Solución:

No se han desarrollado mitigaciones para esta vulnerabilidad, pero desde Cybersecurity and Infrastructure Security Agency (CISA) se recomienda evaluar medias de mitigación como el empleo de buses PLC más cortos para reducir el riesgo de exposición de la información confidencial trasmitida por PLC en remolques.

Detalle:

Los investigadores han descubierto que las comunicaciones mediante PLC que se utilizan para enviar información al sistema ECU (*Engine Control Unit*, unidad de control de motor) pueden ser interceptadas a una distancia de entre un metro y medio y dos metros y medio aproximadamente, aunque se cree que con mejores receptores la distancia puede ser superior.

En la mayoría de los casos esa información es utilizada para comunicar el estado de los frenos y los sistemas ABS, pero la divulgación de vulnerabilidad también pretende evitar que se trasmita otro tipo de información confidencial ante el riesgo de que este sistema pueda ser interceptado.

Se ha reservado el identificador CVE-2020-14514 para esta vulnerabilidad.

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

---

Boletín de seguridad de Siemens de agosto de 2020

Fecha de publicación: 12/08/2020

Importancia: Crítica

Recursos afectados:

- SICAM WEB firmware para SICAM A8000 RTUs, todas las versiones anteriores a la V05.30;
- Automation License Manager 5, todas las versiones;
- Automation License Manager 6, todas las versiones anteriores a la V6.0.8;
- SIMATIC RF350M, todas las versiones;
- SIMATIC RF650M, todas las versiones;
- SIMOTICS CONNECT 400, todas las versiones;
- Desigo CC, versiones 3.X y 4.X;

- Desigo CC Compact, versiones 3.X y 4.X;
- RUGGEDCOM RM1224, todas las versiones anteriores a la V6.3;
- SCALANCE M-800 / S615, todas las versiones anteriores a la V6.3;

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 20 avisos de seguridad, de las cuales 15 son actualizaciones.

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

- 1 vulnerabilidad de neutralización incorrecta de la entrada durante la generación de la página web (Cross-site Scripting);
- 1 vulnerabilidad de autorización incorrecta;
- 1 vulnerabilidad de condición de carrera TOCTOU (Time-of-check Time-of-use);
- 1 vulnerabilidad de control incorrecto de generación de código (Inyección de código);
- 1 vulnerabilidad de copia de búfer sin comprobación del tamaño de entrada (Desbordamiento de búfer clásico).

Para estas vulnerabilidades se han reservado los siguientes identificadores: CVE-2020-15781, CVE-2020-7583, CVE-2019-15126, CVE-2020-10055 y CVE-2020-8597.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Múltiples vulnerabilidades en productos Schneider

Fecha de publicación: 12/08/2020

Importancia: Crítica

Recursos afectados:

- SoMove V2.8.1 y anteriores;
- Harmony® eXLhoist base stations v04.00.02.00 y anteriores:
  - ZARB12W;
  - ZARB12H;
  - ZARB18H;
  - ZARB18W;
  - ZARB18HM;
  - ZARB18WM.
- PowerChute Business Edition software V9.0.x y anteriores;
- Modicon M218 Logic Controller V5.0.0.7 y anteriores;
- Todas las versiones hardware de:
  - spaceLYnk;
  - Wiser for KNX (homeLYnk).
- Schneider Electric Modbus Serial Driver (64 bits) versiones anteriores a V3.20 IE 30;
- Schneider Electric Modbus Serial Driver (32 bits) versiones anteriores a V2.20 IE 30;
- Schneider Electric Modbus Driver Suite, versiones anteriores a V14.15.0.0, utilizado en los siguientes productos:
  - Ecostruxure Control Expert (formalmente conocido como Unity Pro);
  - Unity Loader;
  - EcoStruxure Process Expert (formalmente conocido como Hybrid DCS);
  - EcoStruxure OPC UA Server Expert;
  - OPC Factory Server;
  - Advantys Configuration Software;
  - Modbus Communications DTM (Field Devices);
  - SoMove;
  - Ecostruxure Machine Expert (formalmente conocido como SoMachine);
  - Ecostruxure Machine Expert Basic;
  - Harmony® eXLhoist;
  - EcoStruxure Power Commission.
- SFAPV9601 - APC Easy UPS On-Line Software V2.0 y anteriores.

Descripción:

Schneider ha publicado 8 vulnerabilidades, 3 de severidad media, 3 altas y 2 críticas, que podrían permitir a un atacante llevar a cabo la escalada de privilegios, denegación de servicio, ejecución remota de código, bloqueo del sistema, obtención de la contraseña mediante la fuerza bruta o subida de ficheros ejecutables.

Solución:

Actualizar a:

- SoMove V2.8.2;
- Harmony® eXLhoist base stations V04.00.03.00;
- PowerChute Business Edition software 9.1;
- Modicon M218 Logic Controller Firmware V5.0.0.8;
- SpaceLYnk v2.5.1;
- Wiser for KNX (homeLYnk) v2.5.1;
- Schneider Electric Modbus Serial Driver Suite V14.15.0.0;
- SFAPV9601 - APC Easy UPS On-Line Software V2.1.

Detalle:

Las vulnerabilidades de severidad crítica son del tipo limitación incorrecta del nombre de ruta a un directorio restringido (Path Traversal) y podrían permitir a un atacante la carga de ficheros ejecutables en directorios no especificados mediante el acceso a los métodos

vulnerables "FileUploadServlet" o "SoundUploadServlet". Se han asignado los identificadores CVE-2020-7521 y CVE-2020-7522 para estas vulnerabilidades.

Para el resto de vulnerabilidades de severidad media y alta, se han asignado los siguientes identificadores: CVE-2020-7527, CVE-2019-19193, CVE-2020-7524, CVE-2020-7526, CVE-2020-7525 y CVE-2020-7523.

Etiquetas: Actualización, Infraestructuras críticas, Schneider Electric, Vulnerabilidad

---

Vulnerabilidad en Niagara de Tridium

Fecha de publicación: 12/08/2020

Importancia: Media

Recursos afectados:

- Niagara: versiones 4.6.96.28, 4.7.109.20, 4.7.110.32 y 4.8.0.110,
- Niagara Enterprise Security: versiones 2.4.31, 2.4.45 y 4.8.0.35.

Descripción:

Tridium ha informado de una vulnerabilidad en equipos Niagara mediante la cual un atacante podría provocar un agotamiento de recursos.

Solución:

Tridium ha publicado las siguientes actualizaciones:

- Niágara: 4.9.0.198,
- Niagara Enterprise Security: 4.9.0.60.

Las actualizaciones están disponibles poniéndose en contacto con el canal de soporte del equipo de Tridium.

Detalle:

La vulnerabilidad detectada se produce por un agotamiento del tiempo de espera durante un protocolo de enlace TLS provocando que la conexión no termine. Esto hace que Niagara se cuelgue y requiera un reinicio manual para corregirlo.

Se ha reservado el identificador CVE-2020-14483 para esta vulnerabilidad.

Etiquetas: IoT, SSL/TLS, Vulnerabilidad

Denegación de servicio en Automation Runtime de B&R

Fecha de publicación: 13/08/2020

Importancia: Media

Recursos afectados:

Automation Runtime versiones: anteriores a 4.1x, 4.2x, 4.3x, 4.4x, 4.5x, 4.6x, 4.7x.

Descripción:

R&B ha informado de una vulnerabilidad en Automation Runtime que afecta a su servicio TFTP provocando que un atacante pueda causar una denegación de servicio en el producto.

Solución:

Solucionan esta vulnerabilidad los siguientes parches:

- Anteriores a 4.1x: R&B recomienda actualizar a una versión superior,
- 4.2x: N4 26,
- 4.3x: N4 34,
- 4.4x: F4 45,
- 4.5x: E4 53,
- 4.6x: D4 63 (publicación planeada para Q4 2020),
- 4.7x: A4 73.

Detalle:

La implementación del servicio TFTP en el sistema operativo subyacente que utilizan los dispositivos Automation Runtime, tiene un problema en la gestión de memoria al no liberar memoria previamente asignada, causando que un atacante pueda enviar solicitudes especialmente diseñadas al servicio TFTP, que podrían agotar la memoria del dispositivo.

Se ha reservado el identificador CVE-2020-11637 para esta vulnerabilidad.

Etiquetas: SCADA, Vulnerabilidad

Múltiples vulnerabilidades en Philips SureSigns VS4

Fecha de publicación: 20/08/2020

Importancia: Media

Recursos afectados:

Sistema de monitorización de pacientes Philips SureSigns VS4, versión A.07.107 y anteriores.

Descripción:

Philips, de acuerdo con su política de divulgación coordinada de vulnerabilidades, ha notificado 3 vulnerabilidades, 2 de severidad media y 1 baja, de tipo validación de entrada inadecuada, fuerza de cifrado inadecuada y control de acceso inadecuado.

Solución:

Philips recomienda que los clientes cambien todas las contraseñas del sistema en sus dispositivos con contraseñas únicas para cada uno y que lo aseguren físicamente cuando no esté en uso. También se recomienda a los clientes que consideren reemplazar los dispositivos Philips SureSigns VS4 por una tecnología más nueva.

Detalle:

La explotación exitosa podría permitir que un usuario no autorizado acceda a los controles administrativos y las configuraciones del sistema, lo que permitiría realizar cambios en los elementos de configuración del sistema, haciendo que los datos del paciente se envíen a un destino remoto. Esta vulnerabilidad no afecta la seguridad del paciente.

Etiquetas: Infraestructuras críticas, Sanidad, Vulnerabilidad

---

Múltiples vulnerabilidades en NPort IAW5000A-I/O Series de Moxa

Fecha de publicación: 20/08/2020

Importancia: Alta

Recursos afectados:

NPort IAW5000A-I/O Series, versiones de *firmware* 2.1 o anteriores.

Descripción:

Evgeniy Druzhinin y Ilya Karpov, Rostelecom-Solar, han reportado a Moxa múltiples vulnerabilidades de tipo fijación de sesión, gestión de privilegios inadecuada, requisitos de contraseña débiles, transmisión de texto sin cifrar con información confidencial, restricción inadecuada de intentos de autenticación excesivos y divulgación de información.

Solución:

Actualizar el *firmware* del producto afectado a la versión 2.2.

Detalle:

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante secuestrar la sesión robando las cookies del usuario, realizar solicitudes con privilegios administrativos, utilizar credenciales débiles, almacenar y transmitir en el servidor web las credenciales de servicios de terceros en texto sin formato, utilizar ataques de fuerza bruta para evitar la autenticación en una sesión SSH/Telnet y acceder a información confidencial en el servicio web integrado sin la debida autorización.

Etiquetas: Actualización, Comunicaciones, IoT, Vulnerabilidad

---

Limitación incorrecta del nombre de ruta a un directorio restringido en Advantech iView

Fecha de publicación: 26/08/2020

Importancia: Crítica

Recursos afectados:

iView, versiones 5.7 y anteriores.

Descripción:

KPC, perteneciente a Zero Day Initiative de Trend Micro, reportó esta vulnerabilidad a CISA, de severidad crítica y de tipo limitación incorrecta del nombre de ruta a un directorio restringido (*path traversal*).

Solución:

Actualizar iView a la versión 5.7.02.

Detalle:

El producto afectado es vulnerable a una limitación incorrecta del nombre de ruta a un directorio restringido (*path traversal*), que podría permitir a un atacante crear/descargar archivos arbitrarios, limitar la disponibilidad del sistema y ejecutar código de forma remota. Se ha asignado el identificador CVE-2020-16245 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

Desbordamiento de búfer en LeviStudioU de WECON

Fecha de publicación: 26/08/2020

Importancia: Alta

Recursos afectados:

LeviStudioU, versión 2019-09-21 y anteriores.

Descripción:

Natnael Samson, en colaboración con Zero Day Initiative de Trend Micro, reportó esta vulnerabilidad a CISA, de severidad alta y de tipo desbordamiento de búfer basado en pila (*stack*).

Solución:

WECON es consciente del problema y actualmente está desarrollando una solución. Para obtener más información, se puede contactar con WECON online o por teléfono: 0086-591-87868869-894.

Detalle:

La acción de abrir un archivo de proyecto, especialmente diseñado, podría permitir a un atacante explotar la vulnerabilidad de desbordamiento de búfer y ejecutar código bajo los privilegios de la aplicación. Se ha reservado el identificador CVE-2019-16243 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, Vulnerabilidad

Fallos de cifrado en OpenEnterprise de Emerson

Fecha de publicación: 26/08/2020

Importancia: Baja

Recursos afectados:

Todas las versiones de OpenEnterprise hasta la 3.3.5.

Descripción:

El investigador Roman Lozko de Kaspersky ha descubierto una vulnerabilidad en el cifrado utilizado en OpenEnterprise de Emerson que podría permitir a un atacante obtener las credenciales utilizadas por OpenEnterprise para acceder a dispositivos de campo y sistemas externos.

Solución:

Se recomienda instalar la versión OpenEnterprise 3.3 Service Pack 6 (3.3.6), disponible en el área de descargas de la página de soporte de Emerson.

Detalle:

La vulnerabilidad descubierta se refiere a un cifrado inadecuado en OpenEnterprise que permitiría la obtención de credenciales del mismo. Estas credenciales además podrían obtenerse de manera sencilla por un atacante debido a esta vulnerabilidad. Se ha reservado el identificador CVE-2020-16235 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, SCADA, Vulnerabilidad

Múltiples vulnerabilidades en N-Tron 702-W y N-Tron 702M12-W de Red Lion

Fecha de publicación: 28/08/2020

Importancia: Crítica

Recursos afectados:

- N-Tron 702-W, todas las versiones;
- N-Tron 702M12-W, todas las versiones.

Descripción:

Thomas Weber, investigador de SEC Consult Vulnerability Lab, ha descubierto 5 vulnerabilidades, 3 con severidad crítica y 2 altas, de tipo XSS, CSRF, funcionalidad no documentada (*backdoor*) y uso de componentes de terceros sin mantenimiento.

Solución:

Todos los productos de la serie 702-W de Red Lion pasaron a ser productos discontinuados en 2018 y no se pueden actualizar. El fabricante recomienda que estos productos se utilicen localmente dentro de una red segura.

Detalle:

- El producto afectado es vulnerable debido a una interfaz no documentada que se encuentra en el dispositivo, lo que podría permitir que un atacante ejecutase comandos con privilegios de *root* en el dispositivo. Se ha reservado el identificador CVE-2020-16204 para esta vulnerabilidad.
- El producto afectado es vulnerable a un XSS (*Cross-Site Scripting*) reflejado, que podría permitir a un atacante ejecutar de forma remota código arbitrario y realizar acciones en el contexto del usuario atacado. Se ha reservado el identificador CVE-2020-16210 para esta vulnerabilidad.
- El producto afectado es vulnerable a un XSS (*Cross-Site Scripting*) almacenado, lo que podría permitir que un atacante ejecutase de forma remota código arbitrario para obtener acceso a datos confidenciales. Se ha reservado el identificador CVE-2020-16206 para esta vulnerabilidad.
- El producto afectado es vulnerable a CSRF (*Cross-Site Request Forgery*), lo que podría permitir que un atacante modificase diferentes configuraciones de un dispositivo al engañar a un usuario autenticado para que accediese a un enlace especialmente diseñado. Se ha reservado el identificador CVE-2020-16208 para esta vulnerabilidad.
- El producto afectado es vulnerable debido al uso de componentes de terceros con *software* obsoleto, lo que podría permitir que un atacante obtuviese acceso a información confidencial y tomase el control del dispositivo. Se ha reservado el identificador CVE-2017-16544 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Infraestructuras críticas, Vulnerabilidad