
# Boletín de junio de 2019

## Avisos de Sistemas de Control Industrial

## Evasión de autenticación en servidor web de Ewon

**Fecha de publicación:** 04/06/2019

**Importancia:** Alta

**Recursos afectados:**

- Todos los dispositivos del fabricante que posean un *firmware* desde la versión 12.2 hasta la 13.0.

**Descripción:**

El investigador de seguridad Tijl Deneut, de Howest (UGent), ha reportado esta vulnerabilidad de tipo evasión de autenticación. La explotación exitosa de esta vulnerabilidad permitiría a un atacante realizar lecturas de información sensible.

**Solución:**

- El fabricante recomienda actualizar las versiones de *firmware* afectadas a la versión 13.1s0.

**Detalle:**

- Un atacante no autenticado en el servicio web de los dispositivos afectados podría realizar una evasión de autenticación, con la que obtendría acceso a información sensible. Esta vulnerabilidad no posee impacto sobre usuarios que utilicen la solución Talk2M. Sólo afectaría a usuarios locales de Ewon.

**Etiquetas:** Actualización, Vulnerabilidad

## Gestión incorrecta de autenticación y control de accesos en productos Tecson/GOK

**Fecha de publicación:** 05/06/2019

**Importancia:** Crítica

**Recursos afectados:**

- LX-Net
- LX-Q-Net
- e-litro net
- SmartBox4 LAN
- SmartBox4 pro LAN

**Descripción:**

El investigador Maxim Rupp (rupp.it) ha reportado una vulnerabilidad en los productos de Tecson/GOK que afecta a la forma de gestionar el control de accesos y la autenticación.

**Solución:**

- Actualizar el *firmware* de los dispositivos a una versión posterior a la 6.3.x

**Detalle:**

- La aplicación no gestiona de forma adecuada los accesos a los recursos web, permitiendo el acceso a ciertos recursos sin necesidad de una autenticación. Esta vulnerabilidad permitiría a un atacante remoto acceder a recursos localizados en rutas específicas (URL) del servidor web, sin necesidad de estar autenticado. El acceso directo a estos recursos permite el control total del servidor web, pudiendo realizar cambios en la configuración y los ajustes de los dispositivos, como contraseñas, parámetros o

alertas. Se ha reservado el identificador CVE-2019-12254 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

# Múltiples vulnerabilidades en dispositivos de ABB

**Fecha de publicación:** 05/06/2019

**Importancia:** Alta

**Recursos afectados:**

- Índice de revisión G1 con BSP UN31, versión 1.76 y anteriores, de los siguientes productos:
  - CP620 y CP620-WEB
  - CP630 y CP630-WEB
  - CP635, CP635-B y CP635-WEB
- Versiones desde 1.91 hasta 2.8.0.367 de:
  - PB610 Panel Builder 600
- Índice de revisión B1 con BSP UN30, versión 1.76 y anteriores, de los siguientes productos:
  - CP651
  - CP661
  - CP665
  - CP676
- Índice de revisión A0 con BSP UN30, versión 1.76 y anteriores, de los siguientes productos:
  - CP651-WEB
  - CP661-WEB
  - CP665-WEB
  - CP676-WEB

**Descripción:**

ABB agradece a Xen1thLabs, a Darkmatter Company, a United Arab Emirates y a Abu Dhabi el reporte de la información y pruebas de concepto sobre las vulnerabilidades de tipo componentes de software desactualizado, credenciales embebidas, ausencia de comprobación de firma, cuentas administrativas ocultas, salto de directorio en servidor FTP, ausencia de control en el formato de cadenas enviado a los servidores FTP y HTTP, desbordamiento de búfer basado en pila y evasión de autenticación en el servidor web. Un atacante remoto podría llegar a ejecutar código arbitrario y generar un funcionamiento erróneo en los dispositivos afectados por las vulnerabilidades, si logra la explotación de las mismas.

**Solución:**

El fabricante ha puesto a disposición de los usuarios las siguientes actualizaciones:

- PB610 Panel Builder 600, V2.8.0.424
- BSP UN31 V2.31
- BSP UN30 V2.31

**Detalle:**

- Dispositivos ABB CP635 HMI y CP651 HMI:
  - Disponen de una cuenta de administración embebida en el código, la cual es utilizada en la fase de implantación del HMI. Estas credenciales permitirían a un posible atacante, con acceso a la herramienta de configuración 'Panel Builder 600', utilizarlas para crear nuevas interfaces en el HMI o que modifique las etiquetas de los valores (MODBUS coils) que se mapean en el HMI. Se ha reservado el identificador CVE-2019-7225 para esta vulnerabilidad.
  - Debido a una falta de cifrado en la transmisión de los archivos durante la actualización de los dispositivos, la verificación de las actualizaciones se realiza a través de comparación de hashes de los archivos binarios entre el paquete de actualización y la transmisión final. Un atacante con accesos a la red o al paquete de actualización puede manipular estos ficheros binarios, comprometiendo el dispositivo totalmente. Se ha reservado el identificador CVE-2019-7229 para esta vulnerabilidad.
  - Los dispositivos disponen de componentes de software desactualizados y vulnerables que se encuentran enlazados estáticamente en los archivos de firmware y servicios binarios.
- ABB PB610:
  - Dispone de una cuenta de administración embebida en el código, la cual es utilizada en la fase de implantación del HMI. Estas credenciales permitirían a un posible atacante, con acceso a la herramienta de configuración 'Panel Builder 600', utilizarlas para crear nuevas interfaces en el HMI o que modifique las etiquetas de los valores (MODBUS coils) que se mapean en el HMI. Se ha reservado el identificador CVE-2019-7225 para esta vulnerabilidad.
  - El servidor IDAL HTTP CGI tiene accesible una URL que permite a un atacante saltarse la autenticación y acceder a funciones con privilegios elevados. Se ha reservado el identificador CVE-2019-7226 para esta vulnerabilidad.
  - El servidor IDAL FTP no gestiona de manera correcta las solicitudes de cambio de directorio y un atacante podría acceder a cualquier ruta de ficheros, fuera del ámbito del servidor FTP. Se ha reservado el identificador CVE-2019-7227 para esta vulnerabilidad.
  - El servidor IDAL HTTP y el servidor IDAL FTP no validan de forma correcta las entradas de los usuarios, permitiendo a un atacante corromper la memoria con entradas malformadas, para saltarse la autenticación o para ejecutar código remoto. Se han reservado los identificadores CVE-2019-7228 y CVE-2019-7230 para estas vulnerabilidades.
  - El servidor HTTP es vulnerable a un desbordamiento de búfer. Un atacante remoto puede modificar el campo host en la cabecera de la petición HTTP para provocar un desbordamiento de búfer y sobrescribir la dirección del *Structure Exception Handler* (SEH) con un búfer mayor.

**Etiquetas:** Actualización, Comunicaciones, Vulnerabilidad

# Múltiples vulnerabilidades en productos de Geutebrück

**Fecha de publicación:** 05/06/2019

**Importancia:** Alta

**Recursos afectados:**

Las vulnerabilidades afectan a las siguientes versiones y modelos de Encoder y E2 Series Camera:

- G-Code: Todas las versiones 1.12.0.25 y anteriores.
  - EEC-2XXX
- G-Cam: Todas las versiones 1.12.0.25 y anteriores.
  - EBC-21XX
  - EFD-22XX
  - ETHC-22XX
  - EWPC-22XX

**Descripción:**

Los investigadores Romain Luyer, Guillaume Gronnier de CEIS, junto con Davy Douhine de RandoriSec, han reportado múltiples vulnerabilidades de tipo Cross-site Scripting (XSS) e inyección de comandos de sistema operativo. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código remoto como root y ejecutar código en el navegador del operador de la cámara IP.

**Solución:**

- El fabricante ha publicado una actualización de firmware para los usuarios registrados que mitiga las vulnerabilidades:
  - Versión 1.12.13.2

**Detalle:**

- Un atacante remoto autenticado con acceso a la configuración de eventos podría almacenar código malicioso en el servidor que posteriormente podría ser ejecutado por un usuario legítimo, resultando en una ejecución de código dentro del navegador del usuario. Se ha reservado el identificador CVE-2019-10957 para esta vulnerabilidad.
- Un atacante remoto autenticado podría ejecutar comandos como root mediante un comando URL específicamente diseñado. Se ha reservado el identificador CVE-2019-10956 para esta vulnerabilidad.
- Una incorrecta validación en los parámetros de entrada de usuario podría permitir a un atacante remoto autenticado con acceso a la configuración de red introducir comandos del sistema al servidor, logrando ejecutar código remoto como root. Se ha reservado el identificador CVE-2019-10958 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Múltiples vulnerabilidades en Sentinel LDK de Gemalto

**Fecha de publicación:** 06/06/2019

**Importancia:** Baja

**Recursos afectados:**

- Sentinel LDK todas las versiones anteriores a 7.92

**Descripción:**

El investigador Artem Zinenko de Kaspersky Lab ha reportado múltiples vulnerabilidades del tipo *cookie* sin atributo «HTTPOnly» y comunicaciones en texto claro que afectan a Sentinel LDK de Gemalto. Un atacante remoto podría realizar un ataque *man-in-the-middle* y reemplazar el paquete de idioma de la víctima o el robar la cookie del usuario.

**Solución:**

- Se recomienda actualizar Sentinel LDK a la versión 7.92 la cual soluciona estas vulnerabilidades.

**Detalle:**

- *Cookie* sin atributo «HTTPOnly»: la *cookie* «Hasplm» no posee el atributo «HTTPOnly» lo que podría permitir a un atacante el robo de la *cookie* mediante código javascript. Se ha reservado el identificador CVE-2019-8283 para esta vulnerabilidad.
- Comunicaciones en texto claro: el software Gemalto Admin Control Center emplea comunicaciones en texto claro HTTP para comunicarse con www3.safenet-inc.com para obtener los paquetes de lenguaje. Esto podría permitir a un atacante realizar un ataque *man-in-the-middle* y reemplazar el paquete de lenguaje por uno malicioso. Se ha reservado el identificador CVE-2019-8282 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Múltiples vulnerabilidades en Control FPWIN Pro de Panasonic

**Fecha de publicación:** 07/06/2019

**Importancia:** Alta

**Recursos afectados:**

- FPWIN Pro, versión 7.3.0.0 y anteriores.

**Descripción:**

El investigador kimiya, de 9sg Security Team, en colaboración con Zero Day Initiative, de Trend Micro, ha reportado dos vulnerabilidades de tipo desbordamiento de búfer y acceso a recursos que afectan al software de programación de PLC Control FPWIN Pro de Panasonic. La explotación de estas vulnerabilidades podría permitir a un atacante detener el dispositivo y ejecutar código de manera remota.

**Solución:**

- Panasonic recomienda a los usuarios actualizar FPWIN Pro a la versión 7.3.1.0 o posterior para solucionar estas vulnerabilidades.

**Detalle:**

- Los ficheros de proyecto creados por un atacante y cargados por un usuario autenticado podrían provocar un desbordamiento de búfer que podría dar permitir la ejecución de código de manera remota. Se ha reservado el identificador CVE-2019-6530 para esta vulnerabilidad.
- Estos mismos ficheros podrían provocar errores de acceso a recursos de tipo incompatible (*type confusion*) debido a que el recurso no tiene las propiedades esperadas, pudiendo dar lugar a la ejecución de código de manera remota. Se ha reservado el identificador CVE-2019-6532 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Múltiples vulnerabilidades en Proton Enterprise Building Management System de Optergy

**Fecha de publicación:** 07/06/2019

**Importancia:** Crítica

**Recursos afectados:**

- Proton Enterprise versiones 2.3.0 y anteriores.

**Descripción:**

El investigador Gjoko Krstic de Applied Risk ha reportado vulnerabilidades del tipo revelación de información, falsificaciones de petición en sitios cruzados (CSRF), subida sin restricciones de ficheros peligrosos, redirección a URL maliciosas, funcionalidad oculta, exposición de método o función peligroso y credenciales embebidas en el software que afectan a Proton Enterprise de Optergy, que podrían permitir a un atacante ejecutar código de manera remota, divulgar información del sistema y obtener acceso total del sistema.

**Solución:**

- La solución recomendada del fabricante es actualizar los servidores Optergy a la versión 2.4.5

**Detalle:**

- A través de la funcionalidad de restablecimiento de nombre de usuario de la aplicación, un atacante podría enumerar y revelar todos los usuarios válidos en él sistema, además de poder divulgar información interna del sistema. Se han asignado los identificadores CVE-2019-7272 y CVE-2019-7277 para estas vulnerabilidades.
- La falta de validación de la extensión de archivos durante la carga, podría permitir a un atacante remoto no autenticado cargar archivos con extensiones no validadas y ejecutarlos dentro del directorio al cual se han subido. Se ha asignado el identificador CVE-2019-7274 para esta vulnerabilidad.
- Mediante un backdoor no identificado, un atacante podría obtener acceso al sistema y ejecutar código arbitrario. Se ha asignado el identificador CVE-2019-7276 para esta vulnerabilidad.
- Usuarios sin autenticar podrían usar funciones de clases no declaradas para acceder a ciertos recursos. Se ha asignado el identificador CVE-2019-7278 para esta vulnerabilidad.
- Un atacante podría utilizar credenciales embebidas en el software para enviar mensajes SMS no autorizados a cualquier número de teléfono. Se ha asignado el identificador CVE-2019-7279 para esta vulnerabilidad.
- Para el resto de vulnerabilidades se han asignado CVE-2019-7273 y CVE-2019-7275.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Múltiples vulnerabilidades en productos Siemens

**Fecha de publicación:** 11/06/2019

**Importancia:** Alta

**Recursos afectados:**

- Siveillance VMS 2017 R2, todas las versiones anteriores a la 11.2a
- Siveillance VMS 2018 R1, todas las versiones anteriores a la 12.1a
- Siveillance VMS 2018 R2, todas las versiones anteriores a la 12.2a
- Siveillance VMS 2018 R3, todas las versiones anteriores a la 12.3a
- Siveillance VMS 2019 R1, todas las versiones anteriores a la 13.1a
- SCALANCE X-200, todas las versiones anteriores a la 5.2.4
- SCALANCE X-200IRT, SCALANCE X-300 y SCALANCE X-414-3E, todas las versiones
- SIEMENS LOGO!8
  - 6ED1052-xyyxx-0BA8 del FS:01 al FS:06 / Versión de firmware V1.80.xx y V1.81.xx
  - 6ED1052-xyy08-0BA0 FS:01 / versiones de firmware anteriores a la V1.82.02
- Familia SIMATIC Ident MV420 y MV440

**Descripción:**

El CERT de Siemens e investigadores de cirosec GmbH, Ruhr University of Bochum, Hochschule Augsburg y Pen Test Partners, han detectado múltiples vulnerabilidades que afectan a varios productos de Siemens.

**Solución:**

- Siveillance VMS 2017 R2, actualizar a la versión 11.2a
- Siveillance VMS 2018 R1, actualizar a la versión 12.1a
- Siveillance VMS 2018 R2, actualizar a la versión 12.2a
- Siveillance VMS 2018 R3, actualizar a la versión 12.3a

- Siveillance VMS 2019 R1, actualizar a la versión 13.1a
- SCALANCE X-200, actualizar a la versión 5.2.4

Para el resto de productos afectados, Siemens recomienda la aplicación de las siguientes acciones para mitigar las vulnerabilidades:

- Bloquear el puerto 80/TCP en el cortafuegos externo.
- Restringir el acceso a las configuraciones de backups o ficheros de configuración almacenados en los dispositivos.
- Restringir o deshabilitar los mecanismos para acceder por red a las configuraciones de los dispositivos en el caso de que estos se encuentren habilitados.
- Restringir el acceso al módulo de configuración C-PLUG si se encuentra en uso.
- Proteger la red que permite acceder a los productos afectados.
- Al configurar el bit DISA, evitar los cambios en el proyecto por parte de los usuarios registrados. Consulte las instrucciones de funcionamiento.

**Detalle:**

El tipo de vulnerabilidades publicadas se corresponde con las siguientes:

- Ausencia de autenticación. Se han reservado los identificadores CVE-2019-6581 y CVE-2019-6582 para esta vulnerabilidad.
- Extracción de contraseñas. Se ha reservado el identificador CVE-2019-6567 para esta vulnerabilidad.
- Denegación de servicio. Se ha reservado el identificador CVE-2019-6571 para esta vulnerabilidad.
- Obtención de IDs de inicio de sesión. Se ha reservado el identificador CVE-2019-6584 para esta vulnerabilidad.
- Escalado de privilegios. Se ha reservado el identificador CVE-2019-10925 para esta vulnerabilidad.
- Divulgación de información. Se ha reservado el identificador CVE-2019-10926 para esta vulnerabilidad.

**Etiquetas:** Actualización, Comunicaciones, Siemens, Vulnerabilidad

---

# Gestión incorrecta de los ficheros bajo el estándar DICOM

**Fecha de publicación:** 12/06/2019

**Importancia:** Alta

**Recursos afectados:**

- Todos los dispositivos y productos software que gestionen ficheros bajo el estándar NEMA DICOM (extensión .dcm), versión 1995 hasta 2019b.

**Descripción:**

El investigador Markel Picado Ortiz (d00rt), de Cylera Labs, ha publicado una vulnerabilidad en la gestión de los ficheros bajo el estándar DICOM (*Digital Imaging and Communications in Medicine*). Esta vulnerabilidad permitiría a un atacante modificar ficheros de imágenes médicas de tipo DICOM *.dcm, para insertar código malicioso.

**Solución:**

- Se recomienda implementar una solución de antivirus en todos los sistemas de imágenes médicas, así como seguir las recomendaciones publicadas en un informe publicado por DICOM Security Group.

**Detalle:**

- La vulnerabilidad es explotable mediante la inserción de código ejecutable en el preámbulo de 128 bytes, que forma parte de la cabecera de un fichero de tipo DICOM, pudiendo ser modificado por un atacante para encapsular una cabecera diferente. Este nuevo fichero modificado permitiría a dicho atacante insertar y ejecutar código malicioso en ficheros de tipo imagen médica DICOM, con extensión *.dcm. Se ha asignado el identificador CVE-2019-11687 para esta vulnerabilidad.

**Etiquetas:** Vulnerabilidad

---

# Múltiples vulnerabilidades en Proton Enterprise Building Management System de Optergy

**Fecha de publicación:** 07/06/2019

**Importancia:** Crítica

**Recursos afectados:**

- Proton Enterprise versiones 2.3.0 y anteriores.

**Descripción:**

El investigador Gjoko Krstic de Applied Risk ha reportado vulnerabilidades del tipo revelación de información, falsificaciones de petición en sitios cruzados (CSRF), subida sin restricciones de ficheros peligrosos, redirección a URL maliciosas, funcionalidad oculta, exposición de método o función peligroso y credenciales embebidas en el software que afectan a Proton Enterprise de Optergy, que podrían permitir a un atacante ejecutar código de manera remota, divulgar información del sistema y obtener acceso total del sistema.

**Solución:**

- La solución recomendada del fabricante es actualizar los servidores Optergy a la versión 2.4.5

**Detalle:**

- A través de la funcionalidad de restablecimiento de nombre de usuario de la aplicación, un atacante podría enumerar y revelar todos los usuarios válidos en él sistema, además de poder divulgar información interna del sistema. Se han asignado los

identificadores CVE-2019-7272 y CVE-2019-7277 para estas vulnerabilidades.
- La falta de validación de la extensión de archivos durante la carga, podría permitir a un atacante remoto no autenticado cargar archivos con extensiones no validadas y ejecutarlos dentro del directorio al cual se han subido. Se ha asignado el identificador CVE-2019-7274 para esta vulnerabilidad.
- Mediante un backdoor no identificado, un atacante podría obtener acceso al sistema y ejecutar código arbitrario. Se ha asignado el identificador CVE-2019-7276 para esta vulnerabilidad.
- Usuarios sin autenticar podrían usar funciones de clases no declaradas para acceder a ciertos recursos. Se ha asignado el identificador CVE-2019-7278 para esta vulnerabilidad.
- Un atacante podría utilizar credenciales embebidas en el software para enviar mensajes SMS no autorizados a cualquier número de teléfono. Se ha asignado el identificador CVE-2019-7279 para esta vulnerabilidad.
- Para el resto de vulnerabilidades se han asignado CVE-2019-7273 y CVE-2019-7275.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Múltiples vulnerabilidades en productos Siemens

**Fecha de publicación:** 11/06/2019

**Importancia:** Alta

**Recursos afectados:**

- Siveillance VMS 2017 R2, todas las versiones anteriores a la 11.2a
- Siveillance VMS 2018 R1, todas las versiones anteriores a la 12.1a
- Siveillance VMS 2018 R2, todas las versiones anteriores a la 12.2a
- Siveillance VMS 2018 R3, todas las versiones anteriores a la 12.3a
- Siveillance VMS 2019 R1, todas las versiones anteriores a la 13.1a
- SCALANCE X-200, todas las versiones anteriores a la 5.2.4
- SCALANCE X-200IRT, SCALANCE X-300 y SCALANCE X-414-3E, todas las versiones
- SIEMENS LOGO!8
  - 6ED1052-xyyxx-0BA8 del FS:01 al FS:06 / Versión de firmware V1.80.xx y V1.81.xx
  - 6ED1052-xyy08-0BA0 FS:01 / versiones de firmware anteriores a la V1.82.02
- Familia SIMATIC Ident MV420 y MV440

**Descripción:**

El CERT de Siemens e investigadores de cirosec GmbH, Ruhr University of Bochum, Hochschule Augsburg y Pen Test Partners, han detectado múltiples vulnerabilidades que afectan a varios productos de Siemens.

**Solución:**

- Siveillance VMS 2017 R2, actualizar a la versión 11.2a
- Siveillance VMS 2018 R1, actualizar a la versión 12.1a
- Siveillance VMS 2018 R2, actualizar a la versión 12.2a
- Siveillance VMS 2018 R3, actualizar a la versión 12.3a
- Siveillance VMS 2019 R1, actualizar a la versión 13.1a
- SCALANCE X-200, actualizar a la versión 5.2.4

Para el resto de productos afectados, Siemens recomienda la aplicación de las siguientes acciones para mitigar las vulnerabilidades:

- Bloquear el puerto 80/TCP en el cortafuegos externo.
- Restringir el acceso a las configuraciones de backups o ficheros de configuración almacenados en los dispositivos.
- Restringir o deshabilitar los mecanismos para acceder por red a las configuraciones de los dispositivos en el caso de que estos se encuentren habilitados.
- Restringir el acceso al módulo de configuración C-PLUG si se encuentra en uso.
- Proteger la red que permite acceder a los productos afectados.
- Al configurar el bit DISA, evitar los cambios en el proyecto por parte de los usuarios registrados. Consulte las instrucciones de funcionamiento.

**Detalle:**

El tipo de vulnerabilidades publicadas se corresponde con las siguientes:

- Ausencia de autenticación. Se han reservado los identificadores CVE-2019-6581 y CVE-2019-6582 para esta vulnerabilidad.
- Extracción de contraseñas. Se ha reservado el identificador CVE-2019-6567 para esta vulnerabilidad.
- Denegación de servicio. Se ha reservado el identificador CVE-2019-6571 para esta vulnerabilidad.
- Obtención de IDs de inicio de sesión. Se ha reservado el identificador CVE-2019-6584 para esta vulnerabilidad.
- Escalado de privilegios. Se ha reservado el identificador CVE-2019-10925 para esta vulnerabilidad.
- Divulgación de información. Se ha reservado el identificador CVE-2019-10926 para esta vulnerabilidad.

**Etiquetas:** Actualización, Comunicaciones, Siemens, Vulnerabilidad

---

# Gestión incorrecta de los ficheros bajo el estándar DICOM

**Fecha de publicación:** 12/06/2019

**Importancia:** Alta

**Recursos afectados:**

- Todos los dispositivos y productos software que gestionen ficheros bajo el estándar NEMA DICOM (extensión .dcm), versión 1995 hasta 2019b.

**Descripción:**

El investigador Markel Picado Ortiz (d00rt), de Cylera Labs, ha publicado una vulnerabilidad en la gestión de los ficheros bajo el estándar DICOM (*Digital Imaging and Communications in Medicine*). Esta vulnerabilidad permitiría a un atacante modificar ficheros de imágenes médicas de tipo DICOM *.dcm, para insertar código malicioso.

**Solución:**

- Se recomienda implementar una solución de antivirus en todos los sistemas de imágenes médicas, así como seguir las recomendaciones publicadas en un informe publicado por DICOM Security Group.

**Detalle:**

- La vulnerabilidad es explotable mediante la inserción de código ejecutable en el preámbulo de 128 bytes, que forma parte de la cabecera de un fichero de tipo DICOM, pudiendo ser modificado por un atacante para encapsular una cabecera diferente. Este nuevo fichero modificado permitiría a dicho atacante insertar y ejecutar código malicioso en ficheros de tipo imagen médica DICOM, con extensión *.dcm. Se ha asignado el identificador CVE-2019-11687 para esta vulnerabilidad.

**Etiquetas:** Vulnerabilidad

---

# Múltiples vulnerabilidades en productos de Schneider Electric

**Fecha de publicación:** 12/06/2019

**Importancia:** Alta

**Recursos afectados:**

- PowerSCADA Expert 7.30
- PowerSCADA Expert 7.40
- PowerSCADA Expert 8.0, sin el Service Release 1
- ProClima, todas las versiones anteriores a la 8.0.0

**Descripción:**

Investigadores del equipo de seguridad de NSFOCUS han detectado estas vulnerabilidades de tipo inyección de código, errores de búfer, ruta de búsqueda no controlada y exposición de información sensible que podrían provocar la obtención de información sensible y la ejecución de código remoto.

**Solución:**

Actualizar el firmware:

- ProClima a la versión 8.0.0 o posterior.
- PowerSCADA a la versión 9.0 o posterior.

**Detalle:**

- Mediante inyección de código, un atacante remoto no autenticado podría ejecutar código arbitrario en el sistema objetivo. Se ha reservado el identificador CVE-2019-6823 para esta vulnerabilidad.
- Un atacante remoto no autenticado podría ejecutar código arbitrario en el sistema objetivo gracias a un error de búfer. Se ha reservado el identificador CVE-2019-6824 para esta vulnerabilidad.
- La vulnerabilidad del elemento path de búsqueda no controlada podría permitir la ejecución de código arbitrario a un archivo DLL malicioso con el mismo nombre que cualquier DLL dentro del software de instalación. Se ha reservado el identificador CVE-2019-6825 para esta vulnerabilidad.
- Una vulnerabilidad podría permitir a un usuario local autenticado acceder a las credenciales de usuario de Citect. Se ha asignado el identificador CVE-2019-10981 para esta vulnerabilidad.

**Etiquetas:** Actualización, SCADA, Schneider Electric, Vulnerabilidad

---

# Múltiples vulnerabilidades en WAGO 852 Industrial Managed Switch

**Fecha de publicación:** 14/06/2019

**Importancia:** Crítica

**Recursos afectados:**

- 852-303, versiones anteriores a v1.2.2.S0
- 852-1305, versiones anteriores a v1.1.6.S0
- 852-1505, versiones anteriores a v1.1.5.S0

**Descripción:**

El investigador T. Weber, de SEC Consult Vulnerability Lab, ha descubierto múltiples vulnerabilidades en los *switch* industriales WAGO 852, debidas al uso de librerías y componentes software vulnerables, utilizados en el *firmware* embebido. Estas vulnerabilidades permitirían a un atacante acceder al dispositivo gracias a credenciales y claves privadas embebidas en el *firmware*, así como la explotación de un desbordamiento de búfer, provocando una inestabilidad en los dispositivos afectados.

**Solución:**

El fabricante recomienda a los usuarios que actualicen su *switch* con la última versión de *firmware* disponible:

- 852-303: versión 1.2.2.S0 o posterior.
- 852-1305: versión 1.1.6.S0 o posterior.

- 852-1505: versión 1.1.5.S0 o posterior.

**Detalle:**

- Un atacante con acceso a las credenciales codificadas puede acceder al sistema operativo del *switch* con privilegios de root, lo que permitiría realizar una manipulación del sistema operativo del *switch*. Se ha reservado el identificador CVE-2019-12550 para esta vulnerabilidad.
- Un atacante con acceso a la clave SSH codificada puede interrumpir la comunicación o comprometer el *switch*. Las claves SSH no pueden ser regeneradas por los usuarios, y todos los *switches* utilizan la misma clave. Se ha reservado el identificador CVE-2019-12549 para esta vulnerabilidad.
- Componentes de terceros vulnerables: los productos listados utilizan componentes software de terceros con vulnerabilidades conocidas, cuya explotación exitosa podría permitir a un atacante remoto comprometer el *switch* o causar una situación de una denegación de servicio en él. Los identificadores de varias de estas vulnerabilidades, para cada librería vulnerable utilizada, son:
  - BusyBox 1.12.0: CVE-2013-1813, CVE-2016-2148, CVE-2016-6301, CVE-2011-2716, CVE-2011-5325, CVE-2015-9261, CVE-2016-2147, CVE-2017-16544 etc.
  - GNU glibc 2.8: CVE-2010-0296, CVE-2010-3856, CVE-2012-4412, CVE-2014-4043, CVE-2014-9402, CVE-2014-9761, CVE-2014-9984, CVE-2015-14 etc.

**Etiquetas:** Actualización, Comunicaciones, Vulnerabilidad

---

# Autorización inapropiada en ESM de Johnson Controls

**Fecha de publicación:** 14/06/2019

**Importancia:** Media

**Recursos afectados:**

exacqVision ESM versión 5.12.2 y anteriores, en todos los sistemas Windows a excepción de Windows Server.

**Descripción:**

El investigador @bzyo_ ha descubierto una vulnerabilidad de tipo autorización inapropiada en los productos exacqVision ESM de Johnson Controls. La explotación exitosa de dicha vulnerabilidad podría permitir la ejecución de código malicioso en el sistema.

**Solución:**

Actualizar el producto a la versión 19.03

**Detalle:**

De forma predeterminada se otorgan permisos excesivos a los directorios de cuentas autorizadas en el sistema que tienen pocos privilegios, un atacante podría aprovechar esto para realizar cambios en el archivos de las aplicaciones instaladas o realizar una escalada de privilegios. Se ha reservado el identificador CVE-2019-7588 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Múltiples vulnerabilidades en Alaris Gateway Workstation de BD (Becton, Dickinson and Company)

**Fecha de publicación:** 14/06/2019

**Importancia:** Crítica

**Recursos afectados:**

- Alaris Gateway Workstation versiones 1.0.13, 1.1.3 Build 10, 1.1.3 MR Build 11, 1.1.5, 1.1.6, 1.2 Build 15 y 1.3.0 Build 14.
- Adicionalmente, los siguientes productos en las versiones 2.3.6 y anteriores:
  - Alaris GS.
  - Alaris GH.
  - Alaris CC.
  - Alaris TIVA.

**Descripción:**

El investigador Elad Luz, de CyberMDX, ha descubierto múltiples vulnerabilidades en las Alaris Gateway Workstation de BD (Becton, Dickinson and Company) que podrían permitir a un atacante remoto con acceso a la red, visualizar información sensible del dispositivo, editar configuraciones, ejecutar código remoto o causar una denegación de servicio.

**Solución:**

- Para la vulnerabilidad en Alaris Gateway Workstation:
  - Actualizar al último firmware, versión 1.3.2 o 1.6.1.
  - Controlar los accesos de los usuarios a la red donde se encuentra el producto afectado.
  - Aislar los sistemas que poseen el producto afectado frente a sistemas no legítimos.
- Para la vulnerabilidad de carga de archivos peligrosos de la estación de trabajo Alaris Gateway:
  - Bloquear el protocolo SMB.
  - Segregar la red con el uso de VLAN.
  - Asegurarse de que sólo usuarios legítimos tienen acceso a la red.

**Detalle:**

- La interface de navegación que proporciona Alaris Gateway Workstation no gestiona de manera correcta los accesos a diferentes ficheros con información sensible. Un atacante con conocimiento de la IP de la Alaris, puede aprovechar esta vulnerabilidad para obtener información sobre las configuraciones de dicho dispositivo. Se ha asignado el identificador CVE-2019-10962 para esta vulnerabilidad
- La aplicación no dispone de una restricción adecuada de los ficheros que pueden subirse al dispositivo durante una actualización de firmware. Esta vulnerabilidad permitiría a un atacante subir ficheros con contenido malicioso. Se ha asignado el identificador CVE-2019-10959 para esta vulnerabilidad.

**Etiquetas:** Vulnerabilidad

---

# Vulnerabilidades de desbordamiento de búfer en WebAccess de Advantech

**Fecha de publicación:** 20/06/2019

**Importancia:** Crítica

**Recursos afectados:**

WebAccess/SCADA, versión 8.4.0.

**Descripción:**

Tenable ha reportado a Advantech dos vulnerabilidades de tipo desbordamiento de búfer que afectan a su software WebAccess/SCADA. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto, sin autenticación, la ejecución de código de manera arbitraria.

**Solución:**

Actualizar WebAccess/SCADA a la versión 8.4.1 o posteriores.

**Detalle:**

- Existe una vulnerabilidad en *viewsrv.dll* debido a la validación incorrecta de los datos suministrados por el usuario, antes de copiar los datos a un búfer de pila de tamaño fijo, cuando se procesa una llamada IOCTL 10012 RPC. Se ha asignado el identificador CVE-2019-3953 para esta vulnerabilidad.
- La función *VdBroadWinGetLocalDataLogEx()* en *viewdll1.dll* contiene una vulnerabilidad debido a la validación incorrecta de los datos suministrados por el usuario, antes de copiar los datos a un búfer de pila de tamaño fijo, cuando se procesa un mensaje RPC IOCTL 81024. Se ha asignado el identificador CVE-2019-3954 para esta vulnerabilidad.

**Etiquetas:** Actualización, SCADA, Vulnerabilidad

---

# Múltiples vulnerabilidades en Automation Worx Software Suite de Phoenix Contact

**Fecha de publicación:** 20/06/2019

**Importancia:** Alta

**Recursos afectados:**

Los componentes de Automationworx Software Suite con versión 1.86 y anteriores:

- PC Worx
- PC Worx Express
- Config

**Descripción:**

9sg Security Team ha reportado varias vulnerabilidades de tipo ejecución remota de código por puntero no inicializado, ejecución remota de código por liberación de memoria después de su uso y divulgación de información por lectura fuera de límites en los productos Automationworx de Phoenix Contact.

**Solución:**

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

**Detalle:**

Si un atacante con acceso a un archivo de proyecto de PC Worx o Config , lo manipula y lo intercambia en la estación de trabajo de programación de aplicaciones, podría ejecutar código arbitrario de forma remota. Se han reservado los identificadores CVE-2019-12869, CVE-2019-12870, CVE-2019-12871 para estas vulnerabilidades.

**Etiquetas:** 0day, Vulnerabilidad

---

# Control de acceso incorrecto en las bombas de insulina MiniMed de Medtronic

**Fecha de publicación:** 28/06/2019

**Importancia:** Alta

**Recursos afectados:**

- MiniMed 508 en todas las versiones;
- MiniMed Paradigm 511 en todas las versiones;
- MiniMed Paradigm 512/712 en todas las versiones;
- MiniMed Paradigm 712E en todas las versiones;
- MiniMed Paradigm 515/715 en todas las versiones;
- MiniMed Paradigm 522/722 en todas las versiones;
- MiniMed Paradigm 522K/722K en todas las versiones;
- MiniMed Paradigm 523/723 en la versión 2.4A o anteriores;
- MiniMed Paradigm 523K/723K en la versión 2.4A o anteriores;
- MiniMed Paradigm Veo 554/754 en la versión 2.6A o anteriores;
- MiniMed Paradigm Veo 554CM y 754CM en la versión 2.7A o anteriores.

**Descripción:**

Los investigadores independientes Nathanael Paul, Jay Radcliffe, Barnaby Jack, Billy Rios, Jonathan Butts y Jesse Young han detectado esta vulnerabilidad de criticidad alta. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante modificar o interferir en las configuraciones de la bomba de insulina o controlar la administración de esta.

**Solución:**

Medtronic todavía no ha mitigado esta vulnerabilidad, pero aconseja a los pacientes afectados actualizar su bomba de insulina por un modelo más nuevo.

**Detalle:**

Las bombas de insulina afectadas se comunican con otros dispositivos, por ejemplo glucómetros, utilizando una comunicación inalámbrica RF la cual no implementa correctamente la autenticación o autorización. Un atacante, dentro del radio de acceso, podría acceder a los modelos de bombas afectados y cambiar las dosis establecidas además de interceptar los datos. Se ha reservado el identificador CVE-2019-10964 para esta vulnerabilidad.

**Etiquetas:** Vulnerabilidad