
# Boletín de octubre de 2018

## Avisos de Sistemas de Control Industrial

## Múltiples vulnerabilidades en EMG 12 de Entes

**Fecha de publicación:** 03/10/2018

**Importancia:** Crítica

**Recursos afectados:**

- Firmware de Gateways EMG12 Ethernet Modbus, versión 2.57 y anteriores

**Descripción:**

El investigador Can Demirel de Biznet Bilisim ha reportado varias vulnerabilidades de tipo autentificación impropia y exposición de información que podrían permitir a un atacante el acceso no autorizado o la posiblidad de modificar las configuraciones de los dispositivos.

**Solución:**

- Entes EMG recomienda a los usuarios actualizar a la última versión disponible del firmware.

**Detalle:**

- La aplicación usa una interfaz web donde es posible que un ataque pueda omitir la autentificación con una URL especialmente diseñada. Esto permitiría la ejecución de código de una manera remota. Se ha asignado el identificador CVE-2018-14826 para esta vulnerabilidad.
- Se ha identificado una exposición de información a través de la vulnerabilidad de cadenas de consultas en la interfaz web, lo cual podría permitir a un atacante suplantar a un usuario legítimo y ejecutar código arbitrario. Se ha asignado el identificador CVE-2018-14822 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

## Desbordamiento de búfer en ISPSoft de Delta Electronics

**Fecha de publicación:** 03/10/2018

**Importancia:** Media

**Recursos afectados:**

- ISPSoft versión 3.0.5 y anteriores.

**Descripción:**

Ariele Caltabiano (kimiya) de Zero Day Initiative ha reportado una vulnerabilidad del tipo desbordamiento de búfer que afecta al producto ISPSoft de Delta Electronics y que podría permitir a un atacante la ejecución de código bajo el contexto de la aplicación.

**Solución:**

- Delta Electronics recomienda a los usuarios afectados actualizar ISPSoft a la versión 3.0.6 o superior.

**Detalle:**

- Un potencial atacante podría utilizar un fichero especialmente modificado para hacer que la aplicación, al abrir el archivo, lea más allá del límite asignado a un objeto de la pila, lo que permitiría la ejecución de código bajo el contexto de la aplicación. Se ha reservado el identificador CVE-2018-14800 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

# Múltiples vulnerabilidades en PIStudio de Wecon

**Fecha de publicación:** 03/10/2018

**Importancia:** Crítica

**Recursos afectados:**

- PIStudio

**Descripción:**

El investigador independiente Natnael Samson y Mat Powell de Zero Day Initiative (ZDI) de Trend Micro han identificado varias vulnerabilides de tipo desbordamiento de búfer, lectura y escritura fuera de límites y divulgación de información en el producto PIStudio de Wecon. Un potencial atacante podría ejecutar código arbitrario y divulgar información sensible.

**Solución:**

Las vulnerabilidades han sido publicadas sin parche existente de acuerdo a la política de difusión de ZDI de 120 días.

ZDI propone como medida de prevención que los productos afectados interactúen únicamente con ficheros de confianza.

**Detalle:**

- Desbordamiento de búfer: el manejador de ficheros hsc no valida adecuadamente la longitud de los datos proporcionados por el usuario antes de copiarlos a un búfer de longitud fija. Un potencial atacante podría llegar a ejecutar código arbitrario con privilegios elevados.
- Lectura fuera de límites: la gestión de imágenes dentro de ficheros DAT no se realiza adecuadamente y los datos de usuario no son validados correctamente pudiendo llegar a leer posiciones posteriores al final del objeto. Un potencial atacante podría aprovechar esta vulnerabilidad, junto con otras para conseguir la ejecución de código remoto.
- Escritura fuera de límites: el manejador de ficheros hsc no valida adecuadamente la longitud de los datos proporcionados por el usuario, lo que podría provocar una escritura en posiciones posteriores al límite reservado para el objeto. Así, un potencial atacante podría conseguir la ejecución de código arbitrario.
- Divulgación de información: el procesamiento de ficheros de proyecto no dispone de restricciones a referencias a entidades XML externas (XXE), por lo que un potencial atacante podría utilizar un documento especialmente manipulado y conseguir acceso no autorizado a información específica.

**Etiquetas:** 0day, Vulnerabilidad

# Verificación insuficiente de autenticidad de los datos en Modicon M221 de Schneider Electric

**Fecha de publicación:** 04/10/2018

**Importancia:** Alta

**Recursos afectados:**

- Modicon M221 en todas sus versiones

**Descripción:**

El investigador Eran Goldstein de CRITIFENCE, junto con Schneider Electric, ha identificado una vulnerabilidad de verificación insuficiente de autenticidad de datos en Modicon M221 de Schneider Electric que podría permitir a un atacante provocar un cambio en la configuración IPv4 cuando se acceda remotamente al dispositivo.

**Solución:**

El fabricante recomienda las siguientes medidas:

- Configurar un cortafuegos que bloquee todo el acceso remoto/externo al puerto 502
- Dentro de la aplicación Modicon M221, el usuario debe deshabilitar todos los protocolos que no son usados, especialmente el protocolo de programación, como se describe en la sección ?Configuración de la red Ethernet? de la ayuda en línea de SoMachine Basic. Esto prevendrá la programación remota del PLC M221.

**Detalle:**

- Un atacante podría causar un cambio en la configuración de IPv4 (dirección IP, máscara y gateway) cuando se acceda remotamente al dispositivo debido a una verificación insuficiente de autenticidad de los datos. Se ha reservado el identificador CVE-2018-7798 para esta vulnerabilidad.

**Etiquetas:** Schneider Electric, Vulnerabilidad

# Inyección de comandos en router industrial EDR-810 Series de Moxa

**Fecha de publicación:** 08/10/2018

**Importancia:** Crítica

**Recursos afectados:**

- EDR-810 Series con versión de firmware 4.2 o anterior

**Descripción:**

Moxa ha reportado una vulnerabilidad del tipo de inyección de comandos en el servidor web de los routers EDR-810. La explotación exitosa de esta vulnerabilidad permitiría a un atacante remoto ejecutar comandos en el sistema operativo del dispositivo afectado con permisos de superusuario.

**Solución:**

Moxa ha solucionado esta vulnerabilidad publicando una nueva versión de firmware para el dispositivo afectado.

La nueva versión de firmware puede descargarse desde el siguiente enlace: https://www.moxa.com/support/download.aspx?type=support&id=15851

**Detalle:**

Un atacante remoto podría aprovechar una vulnerabilidad de inyección de comandos en el servidor web de Moxa en los dispositivos afectados para ejecutar comandos en el sistema operativo con privilegios de superusuario mediante el parámetro caname presente en la URI /xml/net_WebCADELETEGetValue. Se ha asignado el identificador CVE-2018-16282 para esta vulnerabilidad.

**Etiquetas:** Actualización, Navegador, Vulnerabilidad

---

# Divulgación de información en PeerVue Web Server de Change Healthcare

**Fecha de publicación:** 08/10/2018

**Importancia:** Baja

**Recursos afectados:**

- PeerVue Web Server todas las versiones hasta la 7.6.2

**Descripción:**

Dan Regalado, de Zingbox, ha reportado una vulnerabilidad del tipo divulgación de información en el producto PeerVue Web Server de Change Healthcare. Un potencial atacante podría obtener información técnica sobre PeerVue Web Server pudiendo utilizarla para un posible ataque posterior.

**Solución:**

Change Healthcare ha lanzado un parche que soluciona esta vulnerabilidad. Los usuarios deben ponerse en contacto con el equipo de asistencia de Change Healthcare para obtener información sobre dicho parche.

**Detalle:**

Un atacante podría aprovechar un fallo en el manejo de errores en las comunicaciones HTTP con el servidor para obtener información técnica. Se ha asignado el identificador CVE-2018-10624 para esta vulnerabilidad.

**Etiquetas:** Vulnerabilidad

---

# Divulgación de información en Vue RIS de Carestream

**Fecha de publicación:** 08/10/2018

**Importancia:** Baja

**Recursos afectados:**

- RIS Client Builds versión 11.2 y anteriores funcionando en un sistema Windows 8.1 con IIS 7.5.

**Descripción:**

El investigador Dan Regalado de Zingbox ha reportado una vulnerabilidad de divulgación de información en el producto Vue RIS de Carestream. Un potencial atacante podría conseguir información filtrada y utilizarla para un posible ataque posterior.

**Solución:**

Carestream ha corregido esta vulnerabilidad en la versión actual del software y ha proporcionado las siguientes soluciones para antiguas versiones que se vean afectadas:

- Para RIS 11.2, que se ejecuta con Windows 8.1 e IIS 7.2:
  - Deshabilitar ?Show debug messages?
  - Habilitar SSL para comunicaciones cliente/servidor

**Detalle:**

Al conectarse con un servidor de Carestream y el servicio Oracle TNS listener no se encuentre disponible, se dará lugar a un error HTTP 500, filtrando información técnica que un atacante podría usar para iniciar un ataque más elaborado. Se ha asignado el identificador CVE-2018-17891.

**Etiquetas:** Vulnerabilidad

# Múltiples vulnerabilidades en productos de Auto-Maskin

**Fecha de publicación:** 08/10/2018

**Importancia:** Alta

**Recursos afectados:**

- Paneles remotos Auto-Maskin RP 210E
- Unidades de control DCU 210E
- Aplicación de monitorización Marine Pro Observer para dispositivos móviles

**Descripción:**

Los investigadores Brian Satira y Brian Olson han reportado varias vulnerabilidades de tipo contraseña embebida, validación incorrecta de comunicaciones y transmisión de datos sensibles en texto plano, que podrían ser aprovechadas de manera remota por un potencial atacante que podría llegar a acceder a las unidades y a los motores que están conectados en red y obtener información sensible que se transmita por la misma.

**Solución:**

Como medida preventiva se aconseja aislar los dispositivos afectados de tal forma que sólo sean accesibles desde redes privadas que hayan sido aseguradas.

**Detalle:**

- **Contraseñas embebidas**: El firmware del dispositivo DCU 210E contiene un servidor *dropbear SSH* no documentado que posee credenciales embebidas. Además, la contraseña es susceptible a ser crackeada con facilidad. Se ha asignado el identificador CVE?2018-5399 para esta vulnerabilidad.
- **Validación incorrecta de comunicaciones**: Los productos Auto-Maskin utilizan un protocolo personalizado no documentado para configurar comunicaciones Modbus con otros dispositivos sin realizar una validación de los mismos. Se ha asignado el identificador CVE?2018-5400 para esta vulnerabilidad.
- **Transmisión de información sensible en texto plano**: Los dispositivos afectados transmiten información sensible del proceso mediante comunicaciones Modbus sin cifrar. Se ha asignado el identificador CVE?2018-5401 para esta vulnerabilidad.
- **Transmisión de información sensible en texto plano**: El servidor web embebido utiliza comunicaciones en texto plano para transmitir el PIN del administrador. Se ha asignado el identificador CVE?2018-5402 para esta vulnerabilidad.

**Etiquetas:** Comunicaciones, Navegador, Vulnerabilidad

# Vulnerabilidad del componente ActiveX de Gigasoft para productos iFix HMI de General Electric

**Fecha de publicación:** 10/10/2018

**Importancia:** Media

**Recursos afectados:**

- iFIX versiones desde 2.0 hasta la 5.0
- iFIX versiones 5.1, 5.5 y 5.8

**Descripción:**

El investigador LiMingzheng de 360 aegis ha reportado esta vulnerabilidad de control inseguro del objeto ActiveX marcado como seguro para *scripting*. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante originar un desbordamiento de búfer.

**Solución:**

El fabricante publicó la versión 5.9 iFIX en junio de 2017 para solucionar este problema en la versión del componente Gigasoft 8.0.

General Electric recomienda a los usuarios usar solamente ActiveX con fuentes de confianza.

**Detalle:**

- **Control inseguro de objeto ActiveX marcado como seguro para *scripting*:** Se han identificado múltiples instancias de esta vulnerabilidad en el objeto ActiveX de terceros proporcionado a General Electric iFIX por Gigasoft. Sólo el uso independiente del paquete de gráficos de Gigasoft fuera del producto iFIX puede exponer a los usuarios a esta vulnerabilidad. El método reportado que afecta a Internet Explorer no está expuesto en el producto iFIX, ni se sabe si es la funcionalidad principal del producto iFIX afectada. Se ha asignado el identificador CVE?2018-17925 para esta vulnerabilidad.

**Etiquetas:** Vulnerabilidad

# Vulnerabilidad de tipo DLL Hijacking en Energy Savings Estimator de Fuji Electric

**Fecha de publicación:** 10/10/2018

**Importancia:** Alta

**Recursos afectados:**

- Fuji Electric Energy Savings Estimator versión 1.0.2.0 y anteriores.

**Descripción:**

El investigador Karn Ganeshen ha reportado esta vulnerabilidad de tipo DLL Hijacking al NCCIC. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante cargar una DLL maliciosa y ejecutar código afectando al funcionamiento del sistema.

**Solución:**

Fuji Electric recomienda actualizar su producto a la versión 1.0.2.1

**Detalle:**

- **DLL Hijacking:** La explotación exitosa de esta vulnerabilidad podría dar acceso al sistema a un atacante, con los mismos privilegios que la aplicación que ejecuta la DLL maliciosa. Se ha reservado el identificador CVE-2018-14812 para esta vulnerabilidad.

**Etiquetas:** Vulnerabilidad

---

# Múltiples vulnerabilidades en productos Siemens

**Fecha de publicación:** 10/10/2018

**Importancia:** Alta

**Recursos afectados:**

- SCALANCE W1750D todas las versiones anteriores a la 8.3.0.1
- ROX II todas las versiones anteriores a 2.12.1
- La familia de CPU SIMANTIC S7-1200 en todas las versiones anteriores a 4.2.3
- SIMATIC S7-1500 (incl. F) todas las versiones anteriores a la 2.5 e incluyendo la 2.0
- Controlador de Software SIMATIC S7-1500, todas las versiones anteriores a la 2.5 e incluyendo la 2.0
- SIMATIC ET-200SP Open Controller todas las versiones anteriores a la 2.0 (incluida la 2.0)
- RUGGEDCOM APE, todas las versiones
- RUGGEDCOM RX1400 VPE, todas las versiones
- SIMATIC Field PG M4, todas las versiones de la BIOS anteriores a la 18.01.09
- SIMATIC Field PG M5, todas las versiones de la BIOS anteriores a la 22.01.06
- SIMATIC IPC227E, todas las versiones
- SIMATIC IPC277E, todas las versiones
- SIMATIC IPC3000 SMART V2, todas las versiones
- SIMATIC IPC327E, todas las versiones
- SIMATIC IPC347E, todas las versiones
- SIMATIC IPC377E, todas las versiones
- SIMATIC IPC427C, todas las versiones
- SIMATIC IPC427D, todas las versiones de la BIOS anteriores a la V17.0X.14
- SIMATIC IPC427E, todas las versiones de la BIOS anteriores a la V21.01.09
- SIMATIC IPC477C, todas las versiones
- SIMATIC IPC547E, todas las versiones
- SIMATIC IPC547G, todas las versiones
- SIMATIC IPC627C, todas las versiones
- SIMATIC IPC627D, todas las versiones
- SIMATIC IPC647C, todas las versiones
- SIMOTION P320-4S, todas las versiones

**Descripción:**

Los investigadores Lisa Fournet y Marl Joos de P3 Communications GmbH, Marcin Dudek, Jacek Gajewski, Kinga Staszkiewicz, Jakub Suchorab, y Joanna Walkiewicz del Centro Nacional de Investigación Nuclear de Polonia, en colaboración con Siemens han reportado múltiples vulnerabilidades de tipo problemas criptográficos, gestión inadecuada de privilegios, CSRF, validación incorrecta de entradas y divulgación de información sensible. La explotación exitosa de estas vulnerabilidades permitiría a un atacante de manera remota acceder a los diferentes dispositivos y ejecutar comandos, obtener información sensible u originar denegaciones de servicio.

**Solución:**

- **Problemas criptográficos**: Siemens proporciona una actualización del firmware 8.3.0.1 y recomienda a los usuarios que actualicen a la nueva versión, descargable desde el siguiente enlace: https://support.industry.siemens.com/cs/us/en/view/109760581. Para reducir el riesgo, Siemens aconseja a los administradores que se restrinja el acceso a la interfaz web en los dispositivos afectados.
- **Gestión inadecuada de privilegios**: Siemens recomienda a sus usuarios actualizar a la nueva versión 2.12.1, descargable desde el siguiente enlace: https://support.industry.siemens.com/cs/us/en/view/109760683. Para reducir el riesgo Siemens recomienda a los administradores que se restrinja el acceso a la red para evitar que los posibles atacantes accedan al puerto 22/TCP.
- **CSRF**: Siemens proporciona una actualización del firmware 4.2.3 y recomienda a los usuarios actualizar lo antes posible. La nueva versión de firmware puede descargarse desde el siguiente enlace: https://support.industry.siemens.com/cs/us/en/view/109741461. Para reducir el riesgo, Siemens recomienda a sus usuarios no realizar navegaciones con el navegador web mientras se encuentran registrados en los dispositivos afectados con permisos de superusuario.
- **Validación incorrecta de entrada**: Siemens proporciona actualizaciones para solucionar esta vulnerabilidad en los diferentes sistemas afectados. En los siguientes enlaces pueden descargarse las actualizaciones para resolver la vulnerabilidad:
  - Controlador de Software SIMATIC S7-1500: https://support.industry.siemens.com/cs/us/en/view/109478528
  - SIMANTIC S7-1500: https://support.industry.siemens.com/cs/us/en/ps/13717/dl

Como medidas preventivas, Siemens proporciona varias recomendaciones:

- Restringir el acceso a la red de los dispositivos afectados
- Aplicar el concepto de ?cell-protection? y ?defense-in-depth?

**Detalle:**

- **Problemas criptográficos**: Un atacante con acceso a la red donde se encuentran los dispositivos afectados podría obtener una

clave de sesión TLS. Si el atacante capturase el tráfico TLS entre un usuario y el dispositivo, podría descifrar dicho tráfico. Se ha asignado el identificador CVE-2017-13099 para esta vulnerabilidad.

- **Gestión inadecuada de privilegios**:
  - Un atacante con acceso de red al puerto 22/TCP y credenciales de usuario con pocos privilegios para el dispositivo afectado podría realizar una escalada de privilegios y obtener privilegios de superusuario. Se ha asignado el identificador CVE-2018-13801 para esta vulnerabilidad.
  - Un atacante con autentificación de acceso a una cuenta de usuario de alto privilegio mediante la interfaz SSH en el puerto 22/TCP podría eludir las restricciones y ejecutar de manera arbitraria comandos. Se ha asignado el identificador CVE-2018-13802 para esta vulnerabilidad.
- **CSRF**: La interfaz web permitiría a un atacante utilizar la técnica de ataque CSRF para engañar a usuarios registrados en el dispositivo afectado utilizando enlaces maliciosos. Un potencial atacante necesitaría la interacción de un usuario autenticado, la explotación exitosa de esta vulnerabilidad permitiría a dicho atacante realizar acciones maliciosas a través de la interfaz web. Se ha asignado el identificador CVE-2018-13800 para esta vulnerabilidad.
- **Validación incorrecta de entrada**: Un atacante podría originar una denegación de servicio en la red enviando una gran cantidad de paquetes especialmente formados al PLC. Esta vulnerabilidad podría ser explotada por un atacante con acceso de red en los sistemas afectados. La explotación exitosa de esta vulnerabilidad, no necesita de privilegios o la interacción de un usuario. Un atacante podría usar esta vulnerabilidad para comprometer la disponibilidad de la red. Se ha asignado el identificador CVE-2018-13805 para esta vulnerabilidad.
- **Divulgación de información sensible** (varias vulnerabilidades): Los sistemas con microprocesadores que utilizan la ejecución especulativa y las extensiones software de Intel (Intel SGX) permitirían la divulgación no autorizada de la información que reside en la caché de datos L1 a un atacante con acceso de usuario local. Se han asignado los identificadores para estas vulnerabilidades: CVE-2018-3615, CVE-2018-3620 y CVE-2018-3646.

**Etiquetas:** Actualización, Siemens, Vulnerabilidad

---

# Múltiples vulnerabilidades en diversos productos de Nuuo

**Fecha de publicación:** 15/10/2018

**Importancia:** Crítica

**Recursos afectados:**

- NVRmini2 y NVRsolo, versión 3.8.0 y anteriores.
- CMS, versión 3.1 y anteriores.

**Descripción:**

Los investigadores Pedro Ribeiro, Ariele Caltabiano (kimiya) de 9SG Security Team y Mat Powell de Trend Micro, han identificado varias vulnerabilidades del tipo desbordamiento de búfer, código de depuración sobrante, uso de valores sin suficiente aleatoriedad, uso de funciones obsoletas, asignación incorrecta de permisos y credenciales embebidas. Un atacante podría conseguir la ejecución remota de código y la modificación de cuentas de usuario.

**Solución:**

- Para NVRmini2 y NVRsolo, actualizar a la versión de firmware 3.9.1.
- Para CMS, actualizar a la versión de firmware 3.3

**Detalle:**

- Aprovechando un desbordamiento de búfer, un atacante no autenticado podría conseguir la ejecución remota de código. Se ha reservado el identificador CVE-2018-1149 para esta vulnerabilidad.
- Un atacante remoto no autenticado podría aprovechar ficheros existentes en el sistema para ganar acceso y modificar datos sensibles de los usuarios. Se ha reservado el identificador CVE-2018-1150 para esta vulnerabilidad.
- Un atacante podría obtener el ID de sesión activa generado por el mecanismo de identificación de sesiones de la aplicación y conseguir la ejecución remota de código. Se ha reservado el identificador CVE-2018-17888 para esta vulnerabilidad.
- Mediante funciones obsoletas e inseguras utilizadas por la aplicación, un atacante podría conseguir la ejecución de código remoto. Se ha reservado el identificador CVE-2018-17890 para esta vulnerabilidad.
- El método de control de cuentas de usuario no inicializa de forma adecuada las características de seguridad de las cuentas de usuario, lo que podría permitir a un atacante la ejecución remota de código. Se ha reservado el identificador CVE-2018-17892 para esta vulnerabilidad.
- Lass cuentas por defecto creadas por la aplicación disponen de credenciales embebidas, lo que podría permitir a un atacante el acceso privilegiado al sistema. Se ha reservado el identificador CVE-2018-17894 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Múltiples vulnerabilidades en TPEditor de Delta Electronics

**Fecha de publicación:** 15/10/2018

**Importancia:** Media

**Recursos afectados:**

- Delta Industrial Automation TPEditor, versión 1.90 y anteriores.

**Descripción:**

El investigador Ariele Caltabiano de 9SG Security Team y Mat Powell, en colaboración con Zero Day Initiative, han reportado varias vulnerabilidades de desbordamiento de búfer y de escritura fuera de límites que afectan a TPEditor de Delta Electronics. Un atacante podría ejecutar código arbitrario y divulgar información sensible.

**Solución:**

Delta Electronics ha publicado la versión 1.91 de TPEditor que soluciona estas vulnerabilidades.

**Detalle:**

- Mediante un fichero especialmente manipulado, un atacante podría aprovechar la falta de validación de los datos de entrada del usuario antes de copiarlos del fichero de proyecto a la pila y, de este modo, conseguir la ejecución remota de código. Se ha asignado el identificador CVE-2018-17929 para esta vulnerabilidad.
- Un atacante podría realizar la ejecución remota de código utilizando un fichero especialmente manipulado para aprovechar la falta de validación de los datos de entrada del usuario y escribir fuera de los límites asignados. Se ha asignado el identificador CVE-2018-17927 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Múltiples vulnerabilidades en LAquis SCADA de LCDS

**Fecha de publicación:** 17/10/2018

**Importancia:** Alta

**Recursos afectados:**

- LAquis SCADA Smart Security Manager, versión 4.1.0.3870 y anteriores.

**Descripción:**

El investigador Mat Powell de Zero Day Initiative (Trend Micro), rgod de 9SG Security Team, Esteban Ruiz de Source Incite, b0nd de @garage4hackers y Ashraf Alharbi en colaboración con Zero Day Initiative, han reportado varias vulnerabilidades de tipo desbordamiento de búfer, escritura y lectura fuera de límites, desreferencia de puntero no confiable y control incorrecto a rutas de directorios restringidos (Path traversal). Con la ejecución exitosa de estas vulnerabilidades, un atacante remoto podría ejecutar código arbitrario, escribir contenido en el sistema de destino o bloquear el sistema.

**Solución:**

LCDS propone a los usuarios actualizar a la versión 4.1.0.4114

**Detalle:**

- Una vulnerabilidad de desreferencia de puntero no confiable podría permitir la ejecución de código de manera remota. Se ha asignado el identificador CVE-2018-17893 para esta vulnerabilidad.
- Se ha identificado una vulnerabilidad de lectura fuera de límites, que podría permitir a un atacante remoto ejecutar código en los productos afectados. Se ha asignado el identificador CVE-2018-17895 para esta vulnerabilidad.
- Vulnerabilidad de desbordamiento de búfer permitiría a un potencial atacante remoto la ejecución de código. Se ha asignado el identificador CVE-2018-17897para esta vulnerabilidad.
- Control incorrecto a rutas de directorios restringidos (path traversal) que podría permitir a un atacante la ejecución remota de código. Se ha asignado el identificador CVE-2018-17899 para esta vulnerabilidad.
- Cuando se procesan los archivos de proyecto, la aplicación falla al validar los datos de entrada del usuario antes de realizar operaciones de escritura en un objeto de la pila. Este hecho, podría permitir a un atacante la ejecución de código en el proceso actual que se está ejecutando. Se ha asignado el identificador CVE-2018-17901 para esta vulnerabilidad.
- Se han identificado varias vulnerabilidades de desbordamiento de búfer que podrían permitir a un atacante la ejecución remota de código. Se ha asignado el identificador CVE-2018-17911 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Múltiples vulnerabilidades en CX-Supervisor de Omron

**Fecha de publicación:** 18/10/2018

**Importancia:** Alta

**Recursos afectados:**

- CX-Supervisor versión 3.4.1.0 y anteriores

**Descripción:**

Los investigadores Mat Powell de Zero Day Initiative de Tend Micro, Ariele Caltabiano de 9SG Security Team y b0nd de @garage4hackers, en colaboración con Zero Day Initiative de Tend Micro han reportado varias vulnerabilidades del tipo restricción incorrecta de operaciones dentro de los límites del búfer de memoria, lectura fuera de límites, uso de recursos después de su liberación y conversión incorrecta de tipos, que afectan al software CX-Supervisor de Omron. Un potencial ataque remoto podría ejecutar código arbitrario en el contexto de la aplicación, corromper objetos o forzar a la aplicación a leer un valor fuera de un array.

**Solución:**

Omron la lanzado la versión 3.4.2 que soluciona estas vulnerabilidades. Los usuarios la pueden descargar en el siguiente enlace: https://www.myomron.com/index.php?action=kb&article=1709.

**Detalle:**

- Incorrecta restricción de operaciones dentro de los límites del búfer de memoria. Un potencial atacante podría manipular un byte específico de los archivos de proyecto y causar una corrupción de memoria en el tratamiento de un objeto específico. Se ha asignado el identificador CVE-2018-17905 para esta vulnerabilidad.

- Lectura fuera de límites. Un potencial atacante podría manipular los archivos de proyecto para forzar a la aplicación a leer un valor fuera del array. Se ha asignado el identificador CVE-2018-17907 para esta vulnerabilidad.
- Uso de recursos después de su liberación. Al procesar los archivos de proyecto, la aplicación no es capaz de verificar si se hace referencia a la memoria liberada, esto podría permitir que un atacante ejecute código en el contexto de la aplicación. Se ha asignado el identificador CVE-2018-17909 para esta vulnerabilidad.
- Conversión incorrecta de tipos. Un potencial atacante podría conseguir la ejecución de código en el contexto de la aplicación aprovechándose de un error de conversión en la lectura de los ficheros de proyecto. Se ha asignado el identificador CVE-2018-17913 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Múltiples vulnerabilidades en ThingsPro IIoT Gateway de Moxa

**Fecha de publicación:** 18/10/2018

**Importancia:** Crítica

**Recursos afectados:**

- ThingsPro Gateway versión 2.1

**Descripción:**

El investigador Alexander Nochvay de Kaspersky Lab ha identificado varias vulnerabilidades de tipo enumeración de usuarios, escalado de privilegios, control de acceso inadecuado, cambio de contraseñas débil, almacenamiento de información sensible en texto claro, ejecución de código de forma remota que afectan al dispositivo ThingsPro Gateway de Moxa. Un potencial atacante remoto podría obtener información sensible, realizar una escalada de privilegios, cambiar las contraseñas o ejecutar código de manera remota.

**Solución:**

Moxa ha liberado la versión 2.3 del firmware del dispositivo que soluciona estas vulnerabilidades.
Para la vulnerabilidad de enumeración de usuarios, Moxa recomienda a los usuarios utilizar contraseñas más robustas siguiendo los siguientes criterios:

- Mínimo 8 caracteres de longitud.
- Utilizar caracteres numéricos.
- Utilizar mayúsculas y minúsculas.
- Utilizar caracteres especiales.

**Detalle:**

- Enumeración de usuarios. Un potencial atacante remoto podría utilizar fuerza bruta para conseguir las contraseñas de los usuarios de la web.
- Escalada de privilegios. Un potencial atacante remoto podría aprovechar esta vulnerabilidad para obtener más privilegios.
- Control de acceso inadecuado. Un potencial atacante remoto podría aprovechar esta vulnerabilidad para obtener más privilegios.
- Uso de funciones inseguras. El sistema de cambio de contraseñas no solicita la contraseña antigua por lo que un potencial atacante remoto podría aprovechar esta vulnerabilidad para cambiar fácilmente las contraseñas.
- Almacenamiento de información sensible en texto claro. La explotación de esta vulnerabilidad permitiría a un atacante remoto adivinar los permisos de token.
- Escalado de privilegios. Un potencial atacante remoto podría obtener privilegios de administrador y conseguir la ejecución de comandos accediendo a la API oculta del token.
- Ejecución remota de código. Un potencial atacante remoto podría realizar la inyección de cadenas de texto y forzar al servidor a ejecutar comandos adicionales.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Vulnerabilidad de elevación de privilegios en CT50-Ex de PEPPERL FUCHS

**Fecha de publicación:** 19/10/2018

**Importancia:** Alta

**Recursos afectados:**

- CT50-Ex

**Descripción:**

El fabricante PEPPERL FUCHS ha detectado una vulnerabilidad en uno de sus productos, por la cual un atacante podría llevar a cabo una elevación de privilegios y obtener acceso a información sensible de los productos afectados.

**Solución:**

El fabricante ha publicado una actualización que resuelve la vulnerabilidad detectada.

- CT50-EX
  - Android 6.0
    - Actualizar a CommonES 4.01.00.4134 o versiones posteriores.
    - Actualizar a la versión ECP 2.30.00.0167 o posteriores (dependiendo de cada caso).
  - Android 4.4
    - Actualizar a versión CommonES 3.17.3445 o posteriores.

**Detalle:**

- **Elevación de privilegios:** El servicio que se ejecuta desde el sistema operativo Android no valida de forma correcta las solicitudes de conexión entrantes, lo que podría permitir a un atacante obtener acceso a las pulsaciones de teclas, contraseñas, información personal identificable, fotos, correos electrónicos, o documentos críticos para la empresa. Se ha asignado el identificador CVE-2018-14825 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Múltiples vulnerabilidades en WebAccess de Advantech

**Fecha de publicación:** 24/10/2018

**Importancia:** Crítica

**Recursos afectados:**

- WebAccess, versión 8.3.1 y anteriores.

**Descripción:**

El investigador Mat Powell de Zero Day Initiative de Trend Micro ha identificado varias vulnerabilidades de tipo desbordamiento de búfer, control externo de nombres de ficheros o rutas, gestión de privilegios inadecuada y salto de directorio que afectan a la solución WebAccess de Advantech. Un potencial atacante remoto podría conseguir la ejecución de código, acceso a ficheros para realizar acciones con privilegios de administrador o borrado de ficheros del sistema.

**Solución:**

Advantech ha liberado la versión 8.3.3 de la solución WebAccess que corrige estas vulnerabilidades.

**Detalle:**

- Desbordamiento de búfer. Un potencial atacante remoto podría aprovechar alguno de los múltiples desbordamientos de búfer existentes para conseguir la ejecución de código arbitrario. Se ha asignado el identificador CVE-2018-14816 para esta vulnerabilidad.
- Control externo de nombres de ficheros o rutas. Un potencial atacante podría aprovechar el control externo de nombres de ficheros o rutas en un componente *dll* para realizar un borrado arbitrario de ficheros cuando se procesa. Se ha asignado el identificador CVE-2018-14820 para esta vulnerabilidad.
- Gestión de privilegios inadecuada. Un potencial atacante remoto podría aprovechar esta vulnerabilidad para realizar acciones sobre el sistema con privilegios de administrador. Se ha asignado el identificador CVE-2018-14828 para esta vulnerabilidad.
- Salto de directorio. Un potencial atacante podría ejecutar código arbitrario valiéndose de esta vulnerabilidad. Se ha asignado el identificador CVE-2018-14806 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Vulnerabilidad en Network Card-MS para UPS de Eaton

**Fecha de publicación:** 25/10/2018

**Importancia:** Alta

**Recursos afectados:**

- Network Card-MS para UPS en su versión LA y anteriores.

**Descripción:**

Eaton ha identificado una posible vulnerabilidad en las tarjetas Network Card-MS, que son utilizadas para monitorizar y gestionar Eaton UPS, con un firmware versión LA o anterior.

**Solución:**

Eaton soluciona esta vulnerabilidad actualizando sus productos con la nueva versión del firmware LB desde la página del fabricante.

**Detalle:**

No se ha hecho pública la vulnerabilidad que afecta al dispositivo.

**Etiquetas:** Vulnerabilidad

---

# Múltiples vulnerabilidades en WebAccess de Advantech

**Fecha de publicación:** 26/10/2018

**Importancia:** Alta

**Recursos afectados:**

- WebAccess, versión 8.3.2 y anteriores.

**Descripción:**

El investigador Mat Powell de Zero Day Initiative de Trend Micro, ha identificado varias vulnerabilidades de tipo control de accesos inadecuado y desbordamiento de búfer que afectan a la solución WebAccess de Advantech que podría permitir a un atacante conseguir la ejecución de código arbitrario.

**Solución:**

Advantech ha liberado la versión 8.3.3 de WebAccess que soluciona estas vulnerabilidades.

**Detalle:**

- Un atacante podría ejecutar código arbitrario aprovechando que el control de accesos esta deshabilitado durante el proceso de instalación de la aplicación. Se ha reservado el identificador CVE-2018-17908 para esta vulnerabilidad.
- Una validación incorrecta de la longitud de los datos de entrada proporcionados por el usuario podría permitir a un atacante provocar un desbordamiento de búfer que le permita una ejecución de código arbitrario. Se ha reservado el identificador CVE-2018-17910 para esta vulnerabilidad.

**Etiquetas:** Vulnerabilidad

---

# Cross-site scripting en Reliance 4 SCADA/HMI de GEOVAP

**Fecha de publicación:** 26/10/2018

**Importancia:** Media

**Recursos afectados:**

- Reliance 4 SCADA/HMI, versión 4.7.3, actualización 3 y anteriores.

**Descripción:**

El investigador independiente Ismail Mert ha reportado una vulnerabilidad del tipo neutralización inadecuada de dato de entrada (cross-site scripting) que podría permitir a un atacante remoto usar un proxy http para inyectar código javascript arbitrario en una solicitud http.

**Solución:**

GEOVAP ha publicado la versión 4.8 que soluciona esta vulnerabilidad.

**Detalle:**

- Un atacante remoto no autorizado podría ser capaz de inyectar código arbitrario. Se ha asignado el identificador CVE-2018-17904 para esta vulnerabilidad.

**Etiquetas:** Actualización, SCADA, Vulnerabilidad

---

# Secuestro de DLL en Schneider Electric Software Update (SESU) de Schneider Electric

**Fecha de publicación:** 29/10/2018

**Importancia:** Alta

**Recursos afectados:**

- Schneider Electric Software Update (SESU), todas las versiones anteriores a la versión 2.2.0. SESU es instalado por el siguiente software de Schneider Electric:
  - Acti 9 Smart Test
  - Altiva rATV320DtmLibrary
  - AltivarDTMLibrary
  - AltivarMachine340DTMLibrary
  - AltivarProcessATV6xxDTMLibrary
  - AltivarProcessATV9xxDTMLibrary
  - Blue
  - CompactNSX Firmware Update
  - Ecodial Advance Calculation
  - eConfigure
  - Ecoreach Software
  - EcoStruxure Modicon Builder
  - eXLhoist Configuration Software
  - Lexium 26 DTM Library
  - Lexium 28 DTM Library
  - Lexium 32 DTM Library
  - LV Motor Starter
  - PowerSCADA Expert
  - Schneider Electric Floating License Manager
  - Schneider Electric License Manager
  - Schneider Electric Motion Sizer
  - Schneider Electric SQL Gateway
  - SoMachine Basic
  - SoMachine Motion Software

- SoMachine Motion Tools V4.3
- SoMachine Software
- SoMove
- SoSafe Configurable
- SoSafe Programmable V2.1
- TeSysDTM
- Unity Loader
- Unity Pro
- Vijeo Citect
- Vijeo Designer
- Vijeo Designer Opti 6.1
- Vijeo XD
- Web Gate Client Files

**Descripción:**

Haojun Hou del ADLab de Venustec, en colaboración con Schneider Electric, ha identificado una vulnerabilidad de tipo secuestro de DLL que podría permitir a un atacante remoto la ejecución de código arbitrario.

**Solución:**

Schneider Electric ha publicado la versión 2.2.0 del software que soluciona la vulnerabilidad.

**Detalle:**

- Una vulnerabilidad de secuestro de DLL podría permitir a un atacante remoto llevar a cabo la ejecución de código arbitrario en el sistema. Se ha asignado el identificador CVE-2018-7799 para esta vulnerabilidad

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

---

# Múltiples vulnerabilidades en M2M ETHERNET y CMS-770 de ABB

**Fecha de publicación:** 30/10/2018

**Importancia:** Alta

**Recursos afectados:**

- M2M ETHERNET Network analyser, con firmware versión 2.22 y anteriores, Ethernet firmware versión 1.01 y anteriores.
- CMS-770 Control Unit, versión 1.71 y anteriores.
- Busch-EnergyMonitor, versión 1.71 y anteriores.

**Descripción:**

El investigador independiente Maxim Rupp, en colaboración con ABB, ha identificado múltiples vulnerabilidades del tipo autentificación incorrecta que afectan a los productos M2M ETHERNET y CMS-770 de ABB. Un potencial atacante podría cargar ficheros o leer la configuración de un dispositivo y hacerse con el control.

**Solución:**

ABB ha actualizado los manuales de los productos afectados y recomienda que los usuarios sigan las instrucciones de actualización recomendadas. Por ahora no hay actualizaciones para los dispositivos afectados.

**Detalle:**

- Un atacante no autenticado podría cargar manualmente un archivo de idioma con expresiones no válidas.
- Un atacante podría leer los archivos de configuración del dispositivo consiguiendo así credenciales con las que poder tomar el control del producto.

**Etiquetas:** Vulnerabilidad