Boletín de septiembre de 2019

Avisos de Sistemas de Control Industrial

Fijación de sesión en Pyxis ES de BectonDickinson

Fecha de publicación: 06/09/2019

Importancia: Alta

Recursos afectados:

- Pyxis Enterprise Server, desde la versión 1.3.4 hasta la 1.6.1;
- Pyxis Enterprise Server con Windows Server, desde la versión 4.4 hasta la 4.12.

Descripción:

BD ha reportado una vulnerabilidad, de tipo fijación de sesión, que afecta al equipamiento Pyxis ES (Enterprise Server). La explotación exitosa de esta vulnerabilidad permitiría al atacante reutilizar una sesión de un usuario previamente autenticado, obteniendo el mismo nivel de privilegios y la posibilidad de acceder a datos médicos de los pacientes.

Solución:

BD ha publicado la versión 1.6.1.1 de Pyxis Enterprise Server para solucionar esta vulnerabilidad.

Detalle:

El producto Pyxis ES tiene una vulnerabilidad de tipo fijación de sesión, debido a una gestión incorrecta del cierre de sesión cuando se ha autenticado un usuario mediante un controlador de dominio. Esta vulnerabilidad permitiría a un atacante reutilizar la sesión del usuario, anteriormente registrado en el sistema, con el fin de conseguir privilegios y acceder al dispositivo. La explotación exitosa de esta vulnerabilidad permitiría obtener información sensible de datos confidenciales de los pacientes. Se ha reservado el identificador CVE-2019-13517 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Crimson de Red Lion Controls

Fecha de publicación: 06/09/2019

Importancia: Alta

Recursos afectados:

- Crimson, versiones 3.0 y anteriores;
- Crimson, versiones 3.1 y anteriores, hasta la versión 3112.00.

Descripción:

Se han reportado múltiples vulnerabilidades del tipo restricción incorrecta del búfer de memoria, gestión incorrecta de punteros de memoria, reutilización de recursos previamente liberados y utilización de claves criptográficas embebidas en Crimson de Red Lion Controls, que podrían permitir a un atacante remoto la ejecución de código, el bloqueo del sistema y el acceso a información protegida.

Solución:

- Actualizar a Crimson 3.1 versión 311200 o posterior.

Detalle:

- Una restricción incorrecta de las operaciones en el búfer de memoria podría permitir a un atacante remoto la ejecución de código. Se ha reservado el identificador CVE-2019-10978 para esta vulnerabilidad.

- Una gestión incorrecta de los punteros podría permitir a un atacante enviar un archivo especialmente diseñado para que el programa maneje mal los punteros. Se ha reservado el identificador CVE-2019-10984 para esta vulnerabilidad.
- El uso de una clave criptográfica embebida en el producto podría permitir a un atacante el acceso a los ficheros de configuración. Se ha reservado el identificador CVE-2019-10990 para esta vulnerabilidad.
- La reutilización de recursos previamente liberados podría permitir a un atacante, mediante un archivo especialmente diseñado, hacer referencia a una ubicación en la memoria que debería estar liberada e inaccesible para la aplicación, permitiendo el acceso a memoria no controlada. Se ha reservado el identificador CVE-2019-10994 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Siemens

Fecha de publicación: 11/09/2019

Importancia: Crítica

Recursos afectados:

- RUGGEDCOM WIN70xx Base Station, todas las versiones;
- RUGGEDCOM WIN72xx Base Station, todas las versions;
- IE/WSN-PA Link WirelessHART Gateway, todas las versiones;
- SIMATIC TDC CP51M1, todas las versiones anteriores a V1.1.7;
- CM 1542-1, todas las versiones;
- CP 1242-7, todas las versiones;
- CP 1243-1, todas las versiones;
- CP 1243-7 LTE EU, todas las versiones;
- CP 1243-7 LTE US, todas las versiones,
- CP 1243-8 IRC, todas las versiones;
- CP 1542SP-1, todas las versiones;
- CP 1542SP-1 IRC, todas las versiones;
- CP 1543-1, todas las versiones;
- CP 1543SP-1, todas las versiones;
- CloudConnect 712, todas las versiones anteriores a V1.1.5;
- ROX II, todas las versiones solo afectadas por CVE-2019-11479;
- RUGGEDCOM RM1224, todas las versiones;
- S7-1500 CPU 1518(F)-4 PN/DP MFP, todas las versiones;
- SCALANCE M800, todas las versiones;
- SCALANCE M875, todas las versiones;
- SCALANCE S615, todas las versiones;
- SCALANCE SC-600, todas las versiones anteriores a V2.0.1;
- SCALANCE W-700 (IEEE802.11n);
- SCALANCE W1700, todas las versiones;
- SCALANCE WLC711, todas las versiones;
- SCALANCE WLC712, todas las versiones;
- SIMATIC ITC1500, todas las versiones;
- SIMATIC ITC1500 PRO, todas las versiones;
- SIMATIC ITC1900, todas las versiones;
- SIMATIC ITC1900 PRO, todas las versiones;
- SIMATIC ITC2200, todas las versiones;
- SIMATIC ITC2200 PRO, todas las versiones;
- SIMATIC MV500, todas las versiones;
- SIMATIC RF166C, todas las versiones;
- SIMATIC RF185C, todas las versiones;
- SIMATIC RF186C, todas las versiones;
- SIMATIC RF186CI, todas las versiones;
- SIMATIC RF188C, todas las versiones;
- SIMATIC RF188CI, todas las versiones;
- SIMATIC RF600R, todas las versiones;
- SIMATIC Teleserver Adapter IE Advanced, todas las versiones;
- SIMATIC Teleserver Adapter IE Basic, todas las versiones;
- SINEMA Remote Connect Server, todas las versiones anteriores a V2.0 SP1;
- SNUMERIK 808D, todas las versiones;
- SNUMERIK 828D, todas las versiones;
- SINUMERIK 840D sl, todas las versiones;
- TIM 1531 IRC, todas las versiones;
- SIMATIC Field PG M4, todas las versiones de BIOS anteriores a V18.01.09;
- SIMATIC Field PG M5, todas las versiones de BIOS anteriores a V22.01.07;
- SIMATIC Field PG M6, todas las versiones de BIOS anteriores a V26.01.05;
- SIMATIC IPC127E, todas las versiones;
- SIMATIC IPC2X7E, 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 BIOS anteriores a V17.0X.16;
- SIMATIC IPC427E, todas las versiones de BIOS anteriores a V21.01.11;
- SIMATIC IPC477C, todas las versiones;
- SIMATIC IPC477D, todas las versiones de BIOS anteriores a V17.0X.16;
- SIMATIC IPC477E, todas las versiones de BIOS anteriores a V21.01.11;
- SIMATIC IPC477E Pro, todas las versiones de BIOS anteriores a V21.01.11;
- SIMATIC IPC527G, todas las versiones;
- SIMATIC IPC547E, todas las versiones;
- SIMATIC IPC547G, todas las versiones;
- SIMATIC IPC627C, todas las versiones;
- SIMATIC IPC627D, todas las versiones de BIOS anteriores a V19.02.12;
- SIMATIC IPC627E, todas las versiones de BIOS anteriores a V25.02.04;

- SIMATIC IPC647C, todas las versiones;
- SIMATIC IPC647D, todas las versiones de BIOS anteriores a V19.01.15;
- SIMATIC IPC647E, todas las versiones de BIOS anteriores a V25.02.04;
- SIMATIC IPC677C, todas las versiones;
- SIMATIC IPC677D, todas las versiones de BIOS anteriores a V19.02.12;
- SIMATIC IPC677E, todas las versiones de BIOS anteriores a V25.02.04;
- SIMATIC IPC827C, todas las versiones;
- SIMATIC IPC827D, todas las versiones de BIOS anteriores a V19.02.12;
- SIMATIC IPC847C, todas las versiones;
- SIMATIC IPC847E, todas las versiones de BIOS anteriores a V25.02.04;
- SIMATIC ITP1000, todas las versiones de BIOS anteriores a V23.01.06;
- SIMATIC S7-1500 CPU S7-1518 PN/DP MFP, todas las versiones;
- SIMATIC S7-1500 CPU S7-1518F-4 PN/DP MFP, todas las versions;
- SIMOTION P320-4E, todas las versiones;
- SIMOTION P320-4S, todas las versiones;
- SINUMERIK 840 D sl, todas las versiones;
- SINUMERIK PCU 50.5, todas las versiones;
- SINUMERIK Panels con integración TCU, todas las versiones;
- SINUMERIK TCU 30.3, todas las versiones.

Descripción:

Se han publicado múltiples vulnerabilidades del tipo ejecución de comandos, evasión de autenticación en aplicación web, Cross-Site Scripting (XSS), denegación de servicio, desbordamiento de búfer, obtención de hash de credenciales, credenciales insuficientemente protegidas y Cross-site request forgery (CSRF) que podrían permitir a un atacante ejecutar código arbitrario, obtener información sensible, modificar la conectividad de un usuario, ejecutar comandos en la aplicación web y modificar, subir o eliminar ficheros en el sistema.

Solución:

Consultar la sección de referencias.

Detalle:

A continuación, se detallan las vulnerabilidades de severidad crítica:

- Mediante el envío de paquetes TCP especialmente diseñados a un dispositivo con una manipulación del Urgent Pointer, un atacante podría ejecutar código arbitrario. Se han asignado los identificadores CVE-2019-12255 y CVE-2019-12260 para esta vulnerabilidad.
- Mediante el envío de paquetes de IPv4 a un dispositivo con una opción especialmente diseñada de IP, un atacante podría ejecutar código arbitrario. Se ha asignado los identificadores CVE-2019-1225 y CVE-2019-12256 para esta vulnerabilidad.

Para el resto de las vulnerabilidades, se han asignado los identificadores: CVE-2019-13923, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2018-1212, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-13918, CVE-2019-13919, CVE-2019-13920, CVE-2019-13922, CVE-2019-12257, CVE-2019-12258, CVE-2019-10937, CVE-2019-12259, CVE-2019-12261, CVE-2019-12262, CVE-2019-12263, CVE-2019-12264, CVE-2019-12265.

Etiquetas: Siemens, Vulnerabilidad

Múltiples vulnerabilidades en productos de Schneider Electric

Fecha de publicación: 11/09/2019

Importancia: Crítica

Recursos afectados:

- MEG6501-0001 - U.motion KNX server;
- MEG6501-0002 - U.motion KNX Server Plus;
- MEG6260-0410 - U.motion KNX Server Plus, Touch 10;
- MEG6260-0415 - U.motion KNX Server Plus, Touch 15;
- TwidoSuite v2.20.11 ejecutado en Windows 7 SP1 32-bit;
- Quantum 140 NOE771x1, versión 6.9 y anteriores.

Descripción:

Se han publicado múltiples vulnerabilidades del tipo Cross-Site Scripting (XSS), control de acceso inadecuado, Server-Side Request Forgery (SSRF), formato de string, control de condiciones inesperadas, ruta de búsqueda no confiable y validación de datos de entrada inadecuados. La explotación de estas vulnerabilidades podría permitir a un atacante ejecutar código arbitrario, obtener información sensible, provocar una condición de denegación de servicio o subir ficheros maliciosos.

Solución:

Aplicar las siguientes actualizaciones:

- MEG6501-0001 - U.motion KNX server actualizar a la versión 1.3.7
- MEG6501-0002 - U.motion KNX Server Plus actualizar a la versión 1.3.7
- MEG6260-0410 - U.motion KNX Server Plus, Touch 10 actualizar a la versión 1.3.7
- MEG6260-0415 - U.motion KNX Server Plus, Touch 15 actualizar a la versión 1.3.7
- Quantum 140 140NOE77101 y Quantum 140 140NOE77111, actualizar a la versión 7.0

En el caso de los equipos TwidoSuite, Schneider indica que han alcanzado el fin de su ciclo de vida y recomienda su sustitución por los equipos Modicon M221 o Modicon PLC.

Detalle:

A continuación, se detallan las vulnerabilidades de severidad crítica y altas:

- La vulnerabilidad del tipo Server-Side Request Forgery (SSRF) podría permitir a un atacante obtener información de configuración del servidor al modificar un URL. Se ha asignado el identificador CVE-2019-6837 para esta vulnerabilidad.
- Se podría producir una condición de denegación de servicio cuando un paquete de IP de más de 65535 bytes es recibido por el

módulo de recepción. Se ha asignado el identificador CVE-2019-6811 para esta vulnerabilidad.
- La vulnerabilidad de control de acceso incorrecto podría permitir al sistema de archivos acceder a un fichero erróneo. Se ha asignado el identificador CVE-2019-6836 para esta vulnerabilidad.
- La vulnerabilidad relacionada con el formato de string podría permitir a un atacante a enviar mensajes especialmente diseñados para provocar la ejecución de comandos. Se ha asignado el identificador CVE-2019-6840 para esta vulnerabilidad.
- La vulnerabilidad del tipo de control de acceso incorrecto podría permitir a un usuario con privilegios bajos la subida de archivos. Se ha asignado el identificador CVE-2019-6839 para esta vulnerabilidad.

Para el resto de las vulnerabilidades se han asignado los identificadores: CVE-2019-6835, CVE-2019-6838 y CVE-2019-6837.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de desbordamiento de enteros en PI SQL Client de OSIsoft

Fecha de publicación: 11/09/2019

Importancia: Alta

Recursos afectados:

PI SQL Client 2018 (PI SQL Client OLEDB 2018).

Descripción:

Se ha identificado una vulnerabilidad, de tipo desbordamiento de enteros, que afecta al componente de interfaz PI SQL Client de OSIsoft. La explotación exitosa de esta vulnerabilidad permitiría a un atacante remoto la ejecución de código o la generación de una condición de denegación de servicio.

Solución:

OSIsoft recomienda actualizar a la versión PI SQL Client 2018 R2 o posterior, disponible a través del portal de cliente de OSIsoft.

Detalle:

Un atacante podría aprovechar esta vulnerabilidad en un componente de terceros para ejecutar código de manera remota en el cliente, con los mismos permisos que el usuario de PI SQL Client. Es necesaria la comunicación con un servidor PI SQL Data Access Server (RTQP Engine) para hacer vulnerable al cliente PI SQL. Se ha asignado el identificado CVE-2019-9765 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en TPEditor de Delta Electronics

Fecha de publicación: 11/09/2019

Importancia: Alta

Recursos afectados:

TPEditor, versión 1.94 y anteriores.

Descripción:

El investigador kimiya, de 9sg Security Team, junto con Zero Day Initiative (ZDI) de Trend Micro, han reportado múltiples vulnerabilidades de tipo desbordamiento de búfer y escritura fuera de límites que afecta al software TPEditor de Delta Electronics. La explotación exitosa de estas vulnerabilidades permitiría a un atacante remoto realizar divulgación de información, ejecución de código remoto o detener la aplicación.

Solución:

Delta Electronics recomienda actualizar a la versión 1.95 para solucionar estas vulnerabilidades.

Detalle:

- Múltiples vulnerabilidades de desbordamiento de búfer basado en pila (*stack*) que pueden ser explotadas al procesar archivos de proyecto especialmente diseñados y que permitirían a un atacante remoto realizar una ejecución de código arbitrario. Se ha reservado el identificador CVE-2019-13540 para esta vulnerabilidad.
- Múltiples vulnerabilidades de desbordamiento de búfer basado en memoria dinámica (*heap*) que pueden ser explotadas al procesar archivos de proyecto especialmente diseñados y que permitirían a un atacante remoto realizar una ejecución de código arbitrario. Se ha reservado el identificador CVE-2019-13536 para esta vulnerabilidad.
- Múltiples vulnerabilidades de escritura fuera de límites que pueden ser explotadas al procesar archivos de proyecto especialmente diseñados y que podrían permitir la ejecución remota de código. Se ha reservado el identificador CVE-2019-13544 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en Intelligent Power Protector (IPP) software de Eaton

Fecha de publicación: 11/09/2019

Importancia: Alta

Recursos afectados:

- Intelligent Power Protector version 1.61 y anteriores.

Descripción:

Eaton ha identificado una vulnerabilidad de criticidad alta en el software Intelligent Power Protector.

Solución:

Actualizar a la versión 1.66 de Intelligent Power Protector. Se recomienda a todos los clientes que utilizan el producto afectado, actualicen a dicha versión disponible en su centro de descargas.

Detalle:

Un atacante podría realizar un salto de directorio o realizar un ataque del tipo *man-in-the-middle*.

Etiquetas: Actualización, Vulnerabilidad

Desbordamiento de búfer en WebAcces/SCADA de Advantech

Fecha de publicación: 11/09/2019

Importancia: Crítica

Recursos afectados:

- Advantech WebAccess/SCADA 8.4.1

Descripción:

Tenable ha descubierto una vulnerabilidad del tipo de desbordamiento de búfer. Un atacante remoto, sin autenticar, podría ejecutar código arbitrario.

Solución:

Actualizar a la versión 8.4.2 y posteriores.

Detalle:

El fallo existe en la función de *GetUserPasswd*, que se encuentra en la librería *BwPAlarm.dll*, debido a una validación incorrecta de los datos proporcionados por el usuario antes de copiarlos en el búfer de tamaño fijo cuando se procesa un mensaje RPC IOCTL 70603. Un atacante remoto, sin autenticar, podría ejecutar código arbitrario. Se ha asignado el identificado CVE-2019-3975 para esta vulnerabilidad.

Etiquetas: Actualización, SCADA, Vulnerabilidad

Vulnerabilidad en IntelliVue WLAN de Philips

Fecha de publicación: 12/09/2019

Importancia: Media

Recursos afectados:

Módulo IntelliVue WLAN (Wireless Local Area Network), versiones A y B.

Descripción:

Philips ha identificado una vulnerabilidad que afecta al módulo IntelliVue WLAN, en sus versiones A y B, utilizado en los equipos IntelliVue Patient Monitors.

Solución:

Philips recomienda sustituir los módulos afectados por la versión C, que en su versión actual de *firmware* (B.00.31), no se encuentra afectada por esta vulnerabilidad. En el caso de la versión A, Philips indica que publicará un parche que solucionará esta vulnerabilidad a finales de 2019. La versión B se encuentra descontinuada.

Detalle:

Un usuario no autorizado, con alto nivel de conocimientos y acceso a la red local del dispositivo, sería capaz de dañar tanto el *firmware* del dispositivo, como el flujo de datos.

Etiquetas: Actualización, Sanidad, Vulnerabilidad

Múltiples vulnerabilidades en productos CODESYS de 3S-Smart Software Solutions GmbH

Fecha de publicación: 13/09/2019

Importancia: Crítica

Recursos afectados:

- Todas las variantes de los siguientes productos CODESYS V3, en todas las versiones anteriores a la 3.5.14.10 que contengan el servidor web (CmpWebServer):
  - CODESYS Control para BeagleBone;
  - CODESYS Control para emPC-A/iMX6;
  - CODESYS Control para IOT2000;
  - CODESYS Control para Linux;
  - CODESYS Control para PFC100;
  - CODESYS Control para PFC200;
  - CODESYS Control para Raspberry Pi;
  - CODESYS Control RTE V3;
  - CODESYS Control RTE V3 (para Beckhoff CX);
  - CODESYS Control Win V3 (también parte de la configuración de CODESYS Development System);
  - CODESYS HMI V3;
  - CODESYS Control V3 Runtime System Toolkit;
  - CODESYS V3 Embedded Target Visu Toolkit;
  - CODESYS V3 Remote Target Visu Toolkit.
- Todas las variantes de los siguientes productos CODESYS Control V3, en todas las versiones desde la 3.5.11.0 hasta la 3.5.15.0, que contengan el servidor OPC UA de CODESYS soportando OPC UA Security:
  - CODESYS Control para BeagleBone;
  - CODESYS Control para emPC-A/iMX6;
  - CODESYS Control para IOT2000;
  - CODESYS Control para Linux;
  - CODESYS Control para PFC100;
  - CODESYS Control para PFC200;
  - CODESYS Control para Raspberry Pi;
  - CODESYS Control RTE V3;
  - CODESYS Control RTE V3 (para Beckhoff CX);
  - CODESYS Control Win V3 (también parte de la configuración de CODESYS Development System);
  - CODESYS Control V3 Runtime System Toolkit.
- CODESYS Development System V3, en sus arquitecturas de 32 y 64 bit, versiones anteriores a 3.5.15.0.
- Servidores CODESYS V2.3 ENI, versiones anteriores a 3.2.2.24.

Descripción:

Se han reportado múltiples vulnerabilidades en varios productos CODESYS de 3S-Smart Software Solutions GmbH. La explotación exitosa de estas vulnerabilidades permitiría a un atacante generar una condición de denegación de servicio, ejecutar código de manera remota, ejecutar o mostrar contenido malicioso de librerías manipuladas o acceder a archivos restringidos.

Solución:

Se recomienda actualizar los equipos a las siguientes versiones de software para resolver estas vulnerabilidades:

- 3.2.2.24;
- 3.5.12.80;
- 3.5.14.10;
- 3.5.15.0.

Detalle:

- Una petición http o https, especialmente diseñada, permitiría a un atacante acceder a ficheros fuera del directorio de trabajo del controlador. Se ha reservado el identificador CVE-2019-13532 para esta vulnerabilidad.
- Una petición http o https, especialmente diseñada, podría provocar un desbordamiento de búfer, lo que permitiría generar una condición de denegación de servicio o la ejecución de código de manera remota. Se ha reservado el identificador CVE-2019-13548 para esta vulnerabilidad.
- El sistema expone contenido de la librería activa sin comprobar su validez, lo que permitiría ejecutar o mostrar contenido de librerías manipuladas. Se ha reservado el identificador CVE-2019-13538 para esta vulnerabilidad.
- Una petición especialmente diseñada de un cliente OPC UA de confianza podría provocar una desreferencia de puntero NULL, pudiendo derivar en una condición de denegación de servicio. Se ha reservado el identificador CVE-2019-13542 para esta vulnerabilidad.
- Una petición específicamente diseñada causaría un desbordamiento de búfer basado en una pila y, como consecuencia, se podría ejecutar código arbitrario en el servidor ENI o provocar una condición de denegación de servicio debido a un fallo en dicho servidor.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en Access Professional Edition de Bosch

Fecha de publicación: 13/09/2019

Importancia: Crítica

Recursos afectados:

- Bosch Access Professional Edition (APE), versión 3.7 y anteriores.

Descripción:

El investigador independiente Oleksii Orekhov, coordinado con Bosch, ha identificado dos vulnerabilidades, una de severidad crítica y otra alta. Un atacante podría revelar información confidencial u obtener privilegios de administrador.

Solución:

Actualizar APE a la versión 3.8 o superior.

Detalle:

- Un atacante no autenticado, con acceso a la red del servidor APE, podría revelar información confidencial u obtener privilegios de administración mediante ingeniería inversa. Se ha asignado el identificador CVE-2019-11898 para esta vulnerabilidad.
- Un atacante no autenticado, con acceso a la red del servidor APE, podría conseguir información confidencial en el cliente a través del protocolo SMB. Se ha asignado el identificador CVE-2019-11899 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Exposición de información en SINEMA Remote Connect Server de Siemens

Fecha de publicación: 18/09/2019

Importancia: Media

Recursos afectados:

SINEMA Remote Connect Server versiones anteriores a 2.0 SP1

Descripción:

Los investigadores Hendrik Derre y Tijl Deneut de HOWEST han reportado una vulnerabilidad del tipo exposición de información que podría permitir a un atacante, no autorizado, acceder a información privilegiada del usuario y del dispositivo.

Solución:

Siemens recomienda actualizar SINEMA Remote Connect Server versión 2.0 SP1 o posterior.

Detalle:

Algunas páginas que solo deberían ser accesibles por un usuario privilegiado pueden ser accesibles por uno que no lo es. Un atacante, con acceso a la red y credenciales válidas para el interfaz web, podría revelar información privilegiada. Dicha información no incluye contraseñas. Se ha asignado el identificador CVE-2019-34623 para esta vulnerabilidad.

Etiquetas: Actualización, Siemens, Vulnerabilidad

Exposición de información en Performance IP Cameras y Performance NVRs de Honeywell

Fecha de publicación: 18/09/2019

Importancia: Media

Recursos afectados:

- Performance IP Cameras:
  - HBD3PR2;
  - H4D3PRV3;
  - HED3PR3;
  - H4D3PRV2;
  - HBD3PR1;
  - H4W8PR2;
  - HBW8PR2;
  - H2W2PC1M;
  - H2W4PER3;
  - H2W2PER3;
  - HEW2PER3;
  - HEW4PER3B;
  - HBW2PER1;
  - HEW4PER2;
  - HEW4PER2B;
  - HEW2PER2;
  - H4W2PER2;
  - HBW2PER2;
  - H4W2PER3;
  - HPW2P1.
- Performance NVRs:
  - HEN08104;
  - HEN08144;
  - HEN081124;
  - HEN16104;
  - HEN16144;
  - HEN16184;
  - HEN16204;
  - HEN162244;
  - HEN16284;
  - HEN16304;
  - HEN16384;
  - HEN32104;
  - HEN321124;
  - HEN32204;
  - HEN32284;
  - HEN322164;

- HEN32304;
- HEN32384;
- HEN323164;
- HEN64204;
- HEN64304;
- HEN643164;
- HEN643324;
- HEN643484;
- HEN04103;
- HEN04113;
- HEN04123;
- HEN08103;
- HEN08113;
- HEN08123;
- HEN08143;
- HEN16103;
- HEN16123;
- HEN16143;
- HEN16163;
- HEN04103L;
- HEN08103L;
- HEN16103L;
- HEN32103L.

Descripción:

El investigador independiente Ismail Bulbil ha reportado una vulnerabilidad, de tipo exposición de información, que permitiría a un atacante obtener la información de configuración del dispositivo afectado.

Solución:

Honeywell ha liberado actualizaciones de firmware para todos los productos afectados, disponibles desde su página web.

Detalle:

El servidor web integrado de los dispositivos afectados permitiría a un atacante remoto obtener datos de configuración web, en formato JSON, para las cámaras IP y las NVRs (Network Video Recorders), a los que se puede acceder sin necesidad de autenticación a través de la red. Se ha reservado el identificador CVE-2019-13523 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en WebAccess de Advantech

Fecha de publicación: 18/09/2019

Importancia: Crítica

Recursos afectados:

WebAccess, versiones 8.4.1 y anteriores.

Descripción:

Los investigadores Peter Cheng de Elextec Security Tech. Co., Ltd. y Mat Powell de Trend Micro's Zero Day Initiative, junto con ADLab de VenusTech, han identificado varias vulnerabilidades de tipo inyección de código, inyección de comandos, desbordamiento de la pila del búfer y autorización impropia, que podrían permitir a un atacante ejecutar código arbitrario, acceder a los archivos y ejecutar acciones con un nivel de privilegios elevado, o borrar archivos en el sistema.

Solución:

Advantech ha liberado la versión 8.4.2 de WebAccessNode para solucionar las vulnerabilidades descritas.

Detalle:

- La ejecución de un *exploit* en la red podría causar un control incorrecto de la generación de código, lo que permitiría la ejecución de código remoto, exfiltración de datos o causar el bloqueo del sistema. Se ha reservado el identificador CVE-2019-13558 para esta vulnerabilidad.
- Múltiples vulnerabilidades de inyección de comandos son causadas por una falta de validación de los datos provistos por el usuario, lo que permitiría la eliminación arbitraria de archivos y la ejecución de código remoto. Se ha reservado el identificador CVE-2019-13552 para esta vulnerabilidad.
- Múltiples vulnerabilidades de desbordamiento de búfer basado en pila son causadas por la falta de validación adecuada de la longitud de los datos provistos por el usuario, lo que podría permitir la ejecución de código remoto. Se ha reservado el identificador CVE-2019-13556 para esta vulnerabilidad.
- Una vulnerabilidad de autorización impropia permitiría a un atacante revelar información sensible y provocar un control incorrecto de la generación de código, lo que podría permitir la ejecución de código remoto o producir el bloqueo del sistema. Se ha reservado el identificador CVE-2019-13550 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Dräger

Fecha de publicación: 19/09/2019

Importancia: Alta

Recursos afectados:

- DrÃ¤ger Infinity Acute Care System, versión VG4.1.1/VG4.0.3 y anteriores.
- DrÃ¤ger Standalone Infinity M540, versión VG4.1.1 y anteriores.

Descripción:

Se han descubierto múltiples vulnerabilidades en varios productos de DrÃ¤ger, de tipo falsificación y manipulación de datos y denegación de servicio distribuido, que podrían causar un reinicio del dispositivo o la pérdida de funcionalidad.

Solución:

DrÃ¤ger recomienda actualizar el software de los dispositivos:

- Infinity Acute Care System, versión VG4.1.2/VG4.0.3 o posterior.
- Standalone Infinity M540, versión VG4.1.2 o posterior.

Detalle:

- Los datos enviados por los dispositivos pueden ser falsificados y manipulados, por lo que afectaría a las redes y nodos de monitorización de datos. A su vez, también pueden falsificarse los datos enviados hacia los dispositivos, por lo que sería posible modificar remotamente algunas configuraciones del dispositivo, si este permite el control remoto a través del Infinity Central Station (ICS).
- Existe una vulnerabilidad de tipo denegación de servicio, causada por una gestión incorrecta del tamaño y cantidad de paquetes entrantes de aplicación. Esta podría causar el reinicio de los dispositivos y su desconexión de la red. Para explotar esta vulnerabilidad, el atacante necesitaría tener acceso físico a un puerto dedicado para la red de los dispositivos. Este ataque también puede suceder cuando el dispositivo se conecta a una red inalámbrica, lo que le causaría un reinicio. Sin embargo, la configuración inalámbrica solo está activa cuando el dispositivo está en transporte.

Etiquetas: Actualización, Sanidad, Vulnerabilidad

Exposición de información en controladores PFC100/PFC200 de WAGO

Fecha de publicación: 19/09/2019

Importancia: Media

Recursos afectados:

- Controladores de las series PFC100 y PFC200 con firmware anterior a la versión 12.

Descripción:

El investigador Nico Jansen de Fachhochschule Aachen ha reportado una vulnerabilidad de criticidad media en productos de WAGO. Un atacante remoto podría identificar el software instalado o revelar información sensible.

Solución:

Actualizar el firmware de los dispositivos a la versión 12 o superior

Detalle:

La vulnerabilidad se debe a la posibilidad de enviar peticiones HTTP específicamente generadas para comprobar la existencia de archivos. Un atacante remoto podría identificar el software instalado o revelar información sensible.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Niagara de Tridium

Fecha de publicación: 20/09/2019

Importancia: Alta

Recursos afectados:

- Niagara AX 3.8u4 (JACE 3e, JACE 6e, JACE 7, JACE-8000);
- Niagara 4.4u3 (JACE 3e, JACE 6e, JACE 7, JACE-8000);
- Niagara 4.7u1 (JACE-8000, Edge 10).

Descripción:

Los investigadores Johannes Eger y Fabian Ullrich, de Secure Mobile Networking Lab, han reportado 2 vulnerabilidades, una de severidad alta y otra media, de tipo exposición de información y autorización inapropiada respectivamente, que permitirían a un atacante local el escalar sus privilegios.

Solución:

Tridium ha publicado las siguientes actualizaciones para solucionar estas vulnerabilidades, disponibles poniéndose en contacto con el canal de soporte de ventas o con el equipo de soporte de Tridium:

- Niagara AX 3.8u4:
  - OS Dist: 2.7.402.2;
  - NRE Config Dist: 3.8.401.1.
- Niagara 4.4u3:

    - OS Dist: 4.4.73.38.1 NRE Config;
    - Dist: 4.4.94.14.1.
- Niagara 4.7u1:
    - OS Dist: (JACE 8000) 4.7.109.16.1;
    - OS Dist (Edge 10): 4.7.109.18.1;
    - NRE Config Dist: 4.7.110.32.1.

Detalle:

- El servicio *QNX procfs* provee acceso a información de procesos y recursos, lo que permitiría a un proceso con menor nivel de privilegios acceder al espacio de direcciones objetivo. Se ha asignado el identificador CVE-2019-8998 para esta vulnerabilidad.
- Una utilidad específica podría permitir a un atacante obtener acceso de lectura a archivos con privilegios. Se ha reservado el identificador CVE-2019-13528 para esta vulnerabilidad.

Etiquetas: Actualización, IoT, Vulnerabilidad

Múltiples vulnerabilidades en productos Moxa

Fecha de publicación: 25/09/2019

Importancia: Crítica

Recursos afectados:

- PT-7528 Series, versión 4.0 y anteriores.
- PT-7828 Series, versión 3.9 y anteriores.
- ioLogik 2500 Series, versión 3.0 y anteriores.
- IOxpress Configuration Utility, versión 2.3.0 y anteriores.
- MB3170 Series, versión 4.0 y anteriores.
- MB3270 Series, versión 4.0 y anteriores.
- MB3180 Series, versión 2.0 y anteriores.
- MB3280 Series, versión 3.0 y anteriores.
- MB3480 Series, versión 3.0 y anteriores.
- MB3660 Series, versión 2.2 y anteriores.
- EDS-G516E Series, versión 5.2 y anteriores.
- EDS-510E Series, versión 5.2 y anteriores.

Descripción:

Los investigadores Ilya Karpov y Evgeniy Druzhinin de Rostelecom-Solar, junto con Georgy Zaytsev y Maxim Kozhevnikov de Positive Technologies, han reportado varias vulnerabilidades que afectan a múltiples productos de Moxa.

Solución:

Moxa ha desarrollado diferentes actualizaciones para los dispositivos afectados, que se pueden descargar desde su centro de soporte técnico.

Detalle:

Los tipos de vulnerabilidades detectadas son los siguientes:

- Desbordamiento de búfer basado en pila.
- Uso de un algoritmo criptográfico inseguro.
- Uso de una clave criptográfica codificada.
- Uso de una contraseña codificada.
- Requisitos de contraseña débiles.
- Exposición de información.
- Utilización de algoritmos criptográficos débiles.
- Almacenamiento de texto claro y transmisión de información confidencial.
- Denegación de servicio.
- Desbordamiento de número entero conduce a un desbordamiento del búfer.
- CSRF (*Cross-site request forgery*).
- Copia de búfer sin verificar el tamaño de la entrada.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Validación incorrecta de entradas en múltiples dispositivos de Yokogawa

Fecha de publicación: 27/09/2019

Importancia: Alta

Recursos afectados:

- Exaopc, desde la versión R1.01.00 hasta la R3.77.00;
- Exaplog, desde la versión R1.10.00 hasta la R3.40.00;
- Exaquantum, desde la versión R1.10.00 hasta la R3.02.00;
- Exaquantum/Batch, desde la versión R1.01.00 hasta la R2.50.40;
- Exasmoc, todas las versiones;
- Exarge, todas las versiones;
- GA10, desde la versión R1.01.01 hasta la R3.05.01;
- InsightSuiteAE, desde la versión R1.01.00 hasta la R1.06.00.

Descripción:

El equipo de Yokogawa ha reportado la vulnerabilidad, de tipo validación incorrecta de entradas, que podría permitir a un atacante local la ejecución de ficheros maliciosos mediante el privilegio de servicio.

Solución:

- Exaopc: actualizar a la versión R3.78.00;
- Exaplog: actualizar a la versión R3.40.00 y aplicar el parche para la R3.40.06;
- Exaquantum: actualizar a la versión R3.15.00;
- Exaquantum/Batch: actualizar a la versión R3.10.00;
- Exasmoc: el soporte de finaliza el 30 de septiembre del 2019, por lo que se recomienda migrar a *Platform for Advanced Control and Estimation*, que es el sucesor de Exasmoc;
- Exarqe: el soporte de finaliza el 30 de septiembre del 2019, por lo que se recomienda migrar a *Platform for Advanced Control and Estimation*, que es el sucesor de Exarqe;
- GA10: actualizar a la versión R3.05.06;
- InsightSuiteAE: actualizar a la versión R1.07.00.

Detalle:

La ruta de servicios en algunas aplicaciones de Yokogawa no está contenida entre comillas y contiene espacios. Esto podría provocar que un atacante local ejecutase un fichero malicioso mediante el privilegio de servicio.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en routers de la serie EDR-810 de Moxa

Fecha de publicación: 30/09/2019

Importancia: Alta

Recursos afectados:

Routers de la serie EDR-810, versiones 5.1 y anteriores.

Descripción:

El investigador Guillaume Lopes de Randorisec ha reportado dos vulnerabilidades de criticidad alta. Un atacante podría ejecutar comandos no autorizados en el router y conseguir información del log.

Solución:

Actualizar a la versión 5.3 o superior.

Detalle:

- Un atacante, sin autorización, podría ejecutar comandos en el router debido a la validación incorrecta de las cuentas Admin y ConfigAdmin en la consola web. Se ha reservado el identificador CVE-2019-10969 para esta vulnerabilidad.
- Un atacante, no autenticado, podría exponer información sensible obtenida mediante el *log*. Se ha reservado el identificador CVE-2019-10963 para esta vulnerabilidad

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad