Boletín de julio de 2019

Avisos de Sistemas de Control Industrial

Validación incorrecta de entrada en KACE Systems Management Appliance (SMA) de Quest

Fecha de publicación: 03/07/2019

Importancia: Baja

Recursos afectados:

- KACE SMA, todas las versiones 8.0.x;
- KACE SMA, todas las versiones 8.1.x;
- KACE SMA, todas las versiones 9.0.x.

Descripción:

El investigador Juan Pablo Lopez Yacubian ha detectado una vulnerabilidad de tipo validación incorrecta de entrada. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario administrativo acceder de forma involuntaria al sistema operativo subyacente del dispositivo.

Solución:

Quest recomienda a los usuarios afectados actualizar a la versión 9.1 o posterior.

Detalle:

Esta vulnerabilidad permite acceso involuntario al dispositivo aprovechando las funciones de las herramientas de solución de problemas ubicadas en la interfaz de usuario del administrador. Se ha reservado el identificador CVE-2019-10973 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Siemens

Fecha de publicación: 09/07/2019

Importancia: Alta

Recursos afectados:

- SIMATIC PCS 7 V8.0 y versiones anteriores,
- SIMATIC PCS 7 V8.1, todas las versiones,
- SIMATIC PCS 7, todas las versiones anteriores a V8.2 SP1 con WinCC V7.4 SP1 Upd11,
- SIMATIC PCS 7, todas las versiones anteriores a V9.0 SP2 con WinCC V7.4 SP1 Upd11,
- SIMATIC WinCC Professional V13, V14 y V15 todas las versiones,
- SIMATIC WinCC Runtime Professional V13, V14 y V5 todas las versiones,
- SIMATIC WinCC V7.2 y versiones anteriores,
- SIMATIC WinCC V7.3, todas las versiones,
- SIMATIC WinCC, todas las versiones anteriores a V7.4 SP1 Upd 11,
- SIMATIC WinCC, todas las versiones anteriores a V7-5 Upd 3,
- SIMATIC RF615R, todas las versiones anteriores a V3.2.1,
- SIMATIC RF68XR, todas las versiones anteriores a V3.2.1,
- SIMATIC Field PG M4, M5 y M6 todas las versiones,
- SIMATIC IPC127E, IPC2X7E, IPC3000 SMART V2, IPC327E, IPC347E, IPC377E, IPC427C, IPC427D, IPC427D, IPC477C, IPC477D, IPC527G, IPC547E, IPC547E, IPC547G, IPC627C, IPC627D, IPC647C, IPC647D, IPC677C, IPC677D, IPC827C, IPC827D, IPC847C, IPC847D y ITP1000 todas las versiones,
- SIMATIC IPC427E, todas las versiones de BIOS anteriores a V21.01.11,
- SIMATIC IPC477E, todas las versiones de BIOS anteriores a V21.01.11,

- SIMATIC IPC627E, todas las versiones de BIOS anteriores a V25.02.04,
- SIMATIC IPC647E, todas las versiones de BIOS anteriores a V25.02.04,
- SIMATIC IPC677E, todas las versiones de BIOS anteriores a V25.02.04,
- SIMATIC IPC847E, todas las versiones de BIOS anteriores a V25.02.04,
- SIMATIC S7-1500 CPU S7-1518-4 PN/DP MFP (MLFB: 6ES7518-4AX00-1AC0), todas las versiones,
- SIMATIC S7-1500 CPU S7-1518F-4 PN/DP MFP (MLFB: 6ES7518-4FX00-1AC0), todas las versiones,
- SIMOTION P320-4E, todas las versiones,
- SIMOTION P320-4S, todas las versiones,
- SINUMERIK 840 D sl (NCU720.3B, NCU730.3B, NCU720.3, NCU730.3), todas las versiones,
- SINUMERIK PCU 50.5, todas las versiones,
- SINUMERIK Panels with integrated TCU, todas las versiones,
- SINUMERIK TCU 30.3, todas las versiones,
- TIA Administrator, todas las versiones anteriores a V1.0 SP1 Upd1,
- Spectrum Power 3 (Corporate User Interface) V3.11 y anteriores,
- Spectrum Power 4 (Corporate User Interface) V4.75,
- Spectrum Power 5 (Corporate User Interface) V5.50 y anteriores,
- Spectrum Power 7 (Corporate User Interface) V2.20 y anteriores,
- SIPROTEC 5 con tipos de dispositivos 6MD85, 6MD86,6MD89, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87,7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86,7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82,7UT85, 7UT86, 7UT87 y 7VE85 con diferentes CPUs (CP300 y CP100) y los correspondientes módulos de comunicación Ethernet, todas las versiones anteriores a V7.90,
- Otros SIPROTEC 5 con tipos de dispositivos con diferente CPU (CP300 y CP100) y sus correspondientes módulos de comunicación Ethernet, todas las versiones,
- SIPROTEC 5 relés con diferetes CPU (CP200) y sus respectivos módulos de comunicación Ethernet, todas las versiones,
- DIGSI 5 engineering software, todas las versiones anteriores a V7.90.

Descripción:

Se han publicado múltiples vulnerabilidades del tipo falta de control en la carga de ficheros al sistema, falta de cifrado robusto en comunicaciones web, acceso a secciones de la microarquitectura que no debería tener un usuario autenticado, evasión de autenticación en aplicación web, Cross-Site Scripting (XSS) y envío de paquetes a medida. La explotación de estas vulnerabilidades podría permitir a un atacante ejecutar código arbitrario, obtener información sensible, ejecutar comandos en la aplicación web y modificar, subir o eliminar ficheros en el sistema.

Solución:

Siemens ha desarrollado diferentes actualizaciones para los dispositivos afectados.

Detalle:

A continuación, se detallan las vulnerabilidades de severidad alta:

- La aplicación web de configuración integrada (TIA Administrator) podría permitir a un atacante ejecutar ciertos comandos de la aplicación sin la autenticación adecuada. Se ha asignado el identificador CVE-2019-10915 para esta vulnerabilidad.
- Un atacante remoto podría enviar paquetes especialmente diseñados por el puerto TCP 443 para cargar o descargar archivos dentro de los archivos del sistema. Se ha asignado el identificador CVE-2019-10930 para esta vulnerabilidad.
- Un atacante remoto podría enviar paquetes especialmente diseñados por el puesto TCP 443, pudiendo provocar una denegación de servicio (DoS). Se ha asignado el identificador CVE-2019-10931 para esta vulnerabilidad.
- La aplicación web SIMATIC WinCC DataMonitor podría permitir a un atacante cargar código arbitrario ASPX, pudiendo afectar a la confidencialidad, integridad y disponibilidad del dispositivo. Se ha asignado el identificador CVE-2019-10935 para esta vulnerabilidad.

Para el resto de vulnerabilidades, se han asignado los identificadores CVE-2011-3389, CVE-2016-6329, CVE-2013-0169, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-10933.

Etiquetas: Actualización, Comunicaciones, Navegador, Privacidad, Siemens, Vulnerabilidad

---

Control de acceso inadecuado en PanelView 5510 de Rockwell Automation

Fecha de publicación: 10/07/2019

Importancia: Alta

Recursos afectados:

Todas las versiones de PanelView 5510, fabricadas antes del 13 de marzo de 2019, que nunca han sido actualizadas a las versiones v4.003, v5.002 o posteriores.

Descripción:

El propio fabricante Rockwell Automation ha reportado una vulnerabilidad de tipo control de acceso inadecuado. La explotación exitosa de esta vulnerabilidad por parte de un atacante remoto, con acceso al dispositivo afectado, le permitiría iniciar el terminal y obtener acceso al sistema de archivos con privilegios de *root*.

Solución:

Para solucionar esta vulnerabilidad, el fabricante recomienda la actualización de sus dispositivos a las siguientes versiones, dependiendo de la versión del PanelView 5510 utilizada:

- Para PanelView 5510 utilizando v4, actualizar a la versión 4.003 o posteriores;
- Para PanelView 5510 utilizando v5, actualizar a la versión 5.002 o posteriores.

Detalle:

Un atacante remoto y no autenticado, con acceso a la pantalla gráfica PanelView 5510, podría iniciar el terminal y obtener acceso al sistema de ficheros del dispositivo con privilegios de *root*. Se ha reservado el identificador CVE-2019-10970 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Credenciales embebidas en DeltaV Smart Switches de Emerson

Fecha de publicación: 10/07/2019

Importancia: Media

Recursos afectados:

- Plataforma de gestión DeltaV Distributed Control System, versiones:
  - 11.3.x;
  - 12.3.x.

Descripción:

El investigador Benjamin Crosasso de Sanofi ha reportado esta vulnerabilidad de criticidad media. Un atacante podría acceder con permisos administrativos a los dispositivos DeltaV Smart Switches.

Solución:

El fabricante recomienda aplicar los parches de actualización, disponibles para usuarios registrados, que se encuentran en el artículo DSN19003 (KBA# NK-1900-0808).

Detalle:

El Smart Switch Command Center no cambia las credenciales de la cuenta de administración de DeltaV Smart Switch después de su puesta en producción. Permaneciendo, por defecto, la contraseña vigente indefinidamente. Se ha reservado el identificador CVE-2018-11691 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de Schneider Electric

Fecha de publicación: 10/07/2019

Importancia: Alta

Recursos afectados:

- Zelio Soft V5.2 y versiones anteriores;
- IGSS versión 14 y anteriores;
- Modicon M580 CPU - BMEP582040, todas las versiones anteriores a V2.90;
- Modicon Ethernet Module BMENOC0301, todas las versiones anteriores a V2.16.

Descripción:

Los investigadores mdm y rgod, de 9SG Security Team, en colaboración con Zero Day Initiative (Trend Micro), han reportado varias vulnerabilidades en dispositivos de Schneider Electric. Un atacante remoto podría permitir la ejecución de código, cierre inesperado o generar una condición de denegación de servicio.

Solución:

- Actualizar Zelio Soft a la versión 5.3,
- Actualizar IGSS a las versiones:
  - 13.0.0.19140,
  - 14.0.0.19120.
- Actualizar Modicon Ethernet Module BMENOC0301 a la versión 2.16,
- Actualizar Modicon M580 ? BMEP582040 a la versión 2.90. Consultar el apartado de Referencias para descargar la actualización adecuada para el modelo afectado.

Detalle:

- Una vulnerabilidad se debe a un error en la restricción de operaciones inapropiadas dentro de los límites del búfer de la memoria. Este error podría causar una denegación de servicio en el servidor FTP del Modicon Ethernet al recibir un comando FTP CWD con una longitud de datos superior a 1020 bytes. Se ha reservado el identificador CVE-2018-7838.
- Una vulnerabilidad de escritura fuera de límites podría causar un fallo en el software al manipular los datos en la base de datos mdb. Se ha reservado el identificador CVE-2019-6827.
- Una vulnerabilidad se debe a un fallo en el uso de recursos después de la liberación de memoria. Un atacante remoto podría realizar ejecución de código de manera arbitraria. Se ha reservado el identificador CVE-2018-6822.

Etiquetas: Actualización, Schneider Electric, Vulnerabilidad

Múltiples vulnerabilidades en CNCSoft de Delta Electronics

Fecha de publicación: 12/07/2019

Importancia: Alta

Recursos afectados:

- CNCSoft ScreenEditor versión 1.00.89 y anteriores.

Descripción:

El investigador Natnael Samson, en colaboración con Zero Day Initiative (Trend Micro), ha reportado vulnerabilidades del tipo desbordamiento de búfer y lectura fuera de límites. La explotación exitosa de estas vulnerabilidades por parte de un atacante remoto, podrían permitir ejecutar código, divulgar información o detener la aplicación.

Solución:

Actualizar a la versión 1.00.94.

Detalle:

- Múltiples vulnerabilidades de desbordamiento de búfer basadas en heap podrían permitir, a un atacante remoto, ejecutar código arbitrario mediante el envío de archivos especialmente diseñados debido a la falta de validación de entrada. Se ha reservado el identificador CVE-2019-10982 para esta vulnerabilidad.
- Múltiples vulnerabilidades de lectura fuera de límites podrían permitir la divulgación de información debido a la falta de validación de los datos de entrada del usuario para el procesamiento de los archivos del proyecto. Se ha reservado el identificador CVE-2019-10992 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en dispositivos Holter 2010 Plus de Philips

Fecha de publicación: 12/07/2019

Importancia: Baja

Recursos afectados:

- Holter 2010 Plus, todas las versiones.

Descripción:

Philips ha detectado una vulnerabilidad de criticidad baja en uno de sus productos. Un atacante podría realizar una escalada de privilegios en el equipo afectado.

Solución:

Philips no ha publicado ninguna actualización que solucione la vulnerabilidad. Recomienda a sus clientes implementar controles de acceso basado en roles para controlar el acceso al sistema.

Detalle:

Se ha identificado una vulnerabilidad que podría permitir que se habiliten opciones del sistema no adquiridas previamente. Un atacante, bajo ciertas condiciones, podría realizar una escalada de privilegios en el sistema. Se ha reservado el identificador CVE-2019-10968 para esta vulnerabilidad.

Etiquetas: Sanidad, Vulnerabilidad

Vulnerabilidad de autenticación inapropiada en Aestiva y Aespire Anesthesia de GE

Fecha de publicación: 15/07/2019

Importancia: Media

Recursos afectados:

GE Aestiva y GE Aespire, versiones 7100 y 7900.

Descripción:

El investigador Elad Luz, de CyberMDX, ha reportado esta vulnerabilidad, de tipo autenticación inapropiada. La explotación exitosa de esta vulnerabilidad permitiría a un potencial atacante remoto modificar los parámetros de los dispositivos afectados.

Solución:

GE recomienda a las organizaciones que posean un dispositivo vulnerable utilizar servidores de terminal seguros en el momento de conectarse a los puertos serie de los dispositivos afectados. GE Healthcare planea proporcionar actualizaciones e información de seguridad adicional sobre esta vulnerabilidad para los usuarios afectados en su web.

Detalle:

Se ha detectado una vulnerabilidad, de tipo autenticación inapropiada, en los dispositivos serie que se conectan a través de un servidor de terminal no seguro, agregado a una configuración de red TCP/IP. Esta vulnerabilidad permitiría a un atacante remoto modificar la configuración del dispositivo y silenciar las alarmas. Se ha asignado el identificador CVE-2019-10966 para esta vulnerabilidad.

Etiquetas: Sanidad, Vulnerabilidad

Evasión de autenticación en múltiples productos de ABB

Fecha de publicación: 16/07/2019

Importancia: Alta

Recursos afectados:

- CCLAS, versiones 6.5 y 6.6, incluyendo las versiones de mantenimiento y *hotfix*.
- Ellipse, desde la versión 8.1 hasta la 8.9, incluyendo las versiones de mantenimiento.
- Ellipse, desde la versión 9.0.0 hasta la 9.0.6.

Descripción:

ABB ha detectado una vulnerabilidad de severidad alta. Un atacante, sin acceso autorizado, podría obtener datos de la aplicación.

Solución:

- Actualizar CCLAS a las versiones 6.6.0.4 y 6.7.
- Actualizar Ellipse a las versiones:
  - 8.5.25;
  - 8.6.25;
  - 8.7.23;
  - 8.8.19;
  - 8.9.19;
  - 9.0.7.

Detalle:

La vulnerabilidad se encuentra en el mecanismo de reporte de informes. Cuando un informe es generado, este es almacenado en el disco, y una URL es creada para acceder al informe desde la interfaz de usuario (UI). Esta URL no emplea las comprobaciones adecuadas para garantizar que el usuario que realiza la solicitud es un usuario autenticado. Esto podría permitir a un atacante, con acceso a la URL, descargar el informe.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en el servidor exacqVision de Johnson Controls

Fecha de publicación: 19/07/2019

Importancia: Media

Recursos afectados:

Servidor exacqVision, versiones 9.6 y 9.8.

Descripción:

El investigador Gjoko Kristic, de Applied Risk, ha reportado esta vulnerabilidad de criticidad media. Un atacante, sin autenticar, podría realizar un escalado de privilegios.

Solución:

Actualizar exacqVision a la versión 19.03.

Detalle:

La vulnerabilidad se debe a que varios servicios disponen de una ruta de servicio sin entrecomillar. Un atacante podría insertar código arbitrario en la ruta raíz del sistema que podría ejecutarse al iniciar la aplicación. Se ha reservado el identificador CVE-2019-7590 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en FR Configurator2 de Mitsubishi Electric

Fecha de publicación: 24/07/2019

Importancia: Alta

Recursos afectados:

FR Configurator2 en la versión 1.16S y anteriores

Descripción:

La empresa Applied Risk ha reportado una vulnerabilidad de tipo XML *External Entity* (XXE) y otra de consumo incontrolado de recursos que afecta al producto FR Configurator2 de Mitsubishi.

Solución:

Mitsubishi Electric recomienda a los usuarios actualizar a la última versión 1.17T

Detalle:

- Los datos de entrada proporcionados al analizador XML no son sanitizados previamente, esto podría permitir a un atacante leer ficheros de forma arbitraria. Se ha reservado el identificador CVE-2019-10976 para esta vulnerabilidad.
- Un atacante podría proporcionar un fichero de proyecto no autorizado (.frc2). Cuando el usuario abre el proyecto, se produce el agotamiento de la CPU provocando que el software deje de responder hasta que se reinicie la aplicación, causando una condición de denegación de servicio. Se ha reservado el identificador CVE-2019-10972 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Desbordamiento de búfer en EnergyPlus de National Renewable Energy Laboratory (NREL)

Fecha de publicación: 24/07/2019

Importancia: Media

Recursos afectados:

- EnergyPlus, versión 8.6.0 y versiones anteriores.

Descripción:

El investigador Karn Ganeshen ha reportado una vulnerabilidad de criticidad media. La explotación exitosa de esta vulnerabilidad permitiría a un atacante la ejecución de código arbitrario o causar una condición de denegación de servicio.

Solución:

Actualizar a la versión de la aplicación (v9.0.1).

Detalle:

La aplicación no posee los mecanismos adecuados para evitar que un controlador de excepciones se sobrescriba con código arbitrario. Un atacante, con acceso a la aplicación, podría ejecutar código arbitrario o causar una condición de denegación de servicio. Se ha reservado el identificador CVE-2019-10974 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en VxWorks de Wind River

Fecha de publicación: 30/07/2019

Importancia: Crítica

Recursos afectados:

- VxWorks:
  - desde la versión 6.5 hasta la versión 6.9.4 ambas incluidas;
  - versión 7 preSR620, SR540 y SR610;
  - versiones de VxWorks que utilizan la pila de red independiente de Interpeak;
  - probablemente todas las versiones discontinuadas.

Descripción:

Se han identificado 11 vulnerabilidades que afectan al RTOS VxWorks de tipo desbordamiento de búfer y corrupción de memoria. Un atacante podría ejecutar código de manera arbitraria, causar una denegación de servicio o una fuga de información. Algunos de los dispositivos que utilizan VxWorks son: dispositivos SCADA, controladores industriales, dispositivos médicos de monitorización, máquinas de resonancia magnética, *firewalls*, teléfonos VoIP e impresoras.

Solución:

Wind River ha publicado la versión 7 SR620 de VxWorks que soluciona estas vulnerabilidades. Para más información acceder a la página oficial de soporte.

Detalle:

Las vulnerabilidades de severidad crítica podrían provocar:

- Un desbordamiento de búfer mediante el envío de paquetes IP/DHCP especialmente diseñados enviados al dispositivo de destino el cual no requiere la ejecución de ninguna aplicación o configuración específica por parte de este. La explotación exitosa podría permitir la ejecución de código arbitrario. Se ha reservado el identificador CVE-2019-12256 para esta vulnerabilidad.
- Una corrupción de memoria mediante el uso erróneo del campo de puntero TCP. Un atacante podría usar este campo para conectarse por el puerto TCP y ejecutar código de manera arbitraria. Se han reservado los identificadores CVE-2019-12255 y CVE-2019-12260 para esta vulnerabilidad.

Para el resto de las vulnerabilidades se han reservado los siguientes identificadores: CVE-2019-12257, CVE-2019-12258, CVE-2019-12261, CVE-2019-12262, CVE-2019-12263, CVE-2019-12264, CVE-2019-12259 y CVE-2019-12265.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Sanidad, SCADA, Vulnerabilidad

---

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

Fecha de publicación: 30/07/2019

Importancia: Alta

Recursos afectados:

- CODESYS Control:
  - para BeagleBone;
  - para emPC-A/iMX6;
  - para IOT2000;
  - para PFC100;
  - para PFC200;
  - para Raspberry Pi;
  - para Linux;
  - RTE V3;
  - RTE V3 (para Beckhoff CX);
  - V3 Runtime System Toolkit;
  - Win V3 (también parte de CODESYS Development System setup);
- CODESYS V3 Simulation Runtime (parte de CODESYS Development System);
- CODESYS HMI V3;
- CODESYS V3 Safety SIL2;
- CODESYS Gateway V3;
- Todas las variantes de CODESYS Development System V3 en versiones anteriores a V3.5.15.0.

Descripción:

Se han identificado múltiples vulnerabilidades de criticidad alta que afectan a múltiples productos CODESYS. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto provocar una condición de denegación de servicio, la ejecución de código arbitrario, revelado de información o la captura de credenciales.

Solución:

3S-Smart Software Solutions GmbH ha desarrollado diferentes actualizaciones para los dispositivos afectados disponibles en su centro de descarga de software

Detalle:

- La gestión de usuarios en línea del sistema CODESYS Runtime puede otorgar acceso incorrecto a los subobjetos, incluso si el usuario conectado no tiene permiso heredado para acceder a ellos. Se ha reservado el identificador CVE-2019-9008 para esta vulnerabilidad.
- El sistema de desarrollo CODESYS puede mostrar o ejecutar contenidos activos maliciosos en la librería de documentación sin verificar primero la validez.
- Una petición especialmente diseñada puede causar un error no controlado en los productos CODESYS afectados. Un atacante remoto podría generar en una condición de denegación de servicio. Se ha reservado el identificador CVE-2019-9009 para esta vulnerabilidad.
- Una petición especialmente diseña enviada por un cliente OPC UA de confianza podría provocar una referencia a un puntero nulo, lo que podría dar lugar a una condición de denegación de servicio.
- Si no se utilizan las comunicaciones CODESYS basadas en cifrado TLS, las credenciales se encuentran insuficientemente protegidas durante el transporte. Un atacante, con acceso a las comunicaciones online del PCL, podría obtener las credenciales del usuario. Se ha reservado el identificador CVE-2019-9013 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Vulnerabilidad en la implementación de red Bus CAN en aviónica

Fecha de publicación: 31/07/2019

Importancia: Alta

Recursos afectados:

Aeronaves que empleen redes Bus CAN.

Descripción:

Rapid7 ha reportado una vulnerabilidad en la implementación de la red Bus CAN en las aeronaves. Esta vulnerabilidad podría permitir a un atacante, con acceso físico a la aeronave, inyectar datos falsos dando lugar a lecturas incorrectas en los sistemas de aviónica.

Solución:

Se recomienda tomar las siguientes medidas:

- A los propietarios de aeronaves: restringir el acceso a los aviones en la medida de lo posible.
- A los fabricantes de aeronaves: revisar la implementación de las redes Bus CAN para compensar el vector de ataque físico. La industria de la automoción ha avanzado en la implementación de salvaguardas que impiden ataques físicos similares a los sistemas de Bus CAN. Se deberían evaluar medidas de seguridad como el filtrado, la utilización de listas lista blancas o la segregación específica de la red Bus CAN.

Detalle:

Un atacante con acceso físico a la aeronave podría conectar un dispositivo a la red Bus CAN y utilizarlo para inyectar datos falsos, lo que daría como resultado lecturas incorrectas en los sistemas de aviónica de la aeronave. Los investigadores han señalado que las lecturas de telemetría del motor, la brújula, altitud, la velocidad del aire, y el ángulo de ataque podrían ser manipulados para enviar mediciones

falsas al piloto, lo que podría provocar la pérdida de control de la aeronave afectada.

Etiquetas: Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en FlexAir de Prima Systems

Fecha de publicación: 31/07/2019

Importancia: Crítica

Recursos afectados:

Prima FlexAir, versión 2.3.38 y anteriores.

Descripción:

El investigador Gjoko Krstic, de Applied Risk, ha reportado varias vulnerabilidades del tipo inyección de comandos de sistema operativo, carga sin restricciones de ficheros maliciosos, CSRF, espacio pequeño de valores aleatorios, XSS, exposición de ficheros de respaldo a usuarios sin autorización, autenticación inadecuada y uso de credenciales embebidas. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto la ejecución de comandos de sistema operativo, carga de ficheros maliciosos, ejecutar acciones con permisos de administrador, ejecución de código arbitrario en el navegador del usuario, obtener las credenciales de acceso, evadir la autenticación y tener acceso completo al sistema.

Solución:

Prima Systems ha publicado la versión 2.5.12 de FlexAir para solucionar estas vulnerabilidades.

Detalle:

A continuación, se detallan las vulnerabilidades de mayor criticidad:

- Inyección de comandos de sistema operativo: la aplicación neutraliza de manera incorrecta elementos especiales que permitirían modificar el comando del sistema operativo deseado cuando se envía a un componente posterior, lo que podría permitir a un atacante la ejecución de comandos directamente en el sistema operativo. Se ha asignado el CVE-2019-7670 para esta vulnerabilidad.
- Carga sin restricciones de ficheros maliciosos:
  - La validación inadecuada de la extensión de los ficheros durante la carga de los mismos permitirían a un atacante remoto autenticado la carga y ejecución de aplicaciones maliciosas dentro de la raíz del aplicativo web con privilegios de administrador. Se ha asignado el identificador CVE-2019-7669 para esta vulnerabilidad.
  - La aplicación permite la carga de *scripts* arbitrarios de Python durante la configuración del controlador central principal. Estos *scripts* se pueden ejecutar inmediatamente como administrador y no como usuario del servidor web, lo que le permitiría a un atacante autenticado obtener acceso completo al sistema. Se ha asignado el identificador CVE-2019-9189 para esta vulnerabilidad.
- Exposición de ficheros de respaldo a usuarios sin autorización: la aplicación crea los ficheros de la base de datos de respaldo con nombres predecibles, pudiendo un atacante predecir el nombre del fichero mediante un ataque de fuerza bruta. Un atacante podría explotar esta vulnerabilidad y obtener el fichero de base de datos con la información de inicio de sesión, pudiendo evadir la autenticación y obtener acceso completo al sistema. Se ha asignado el identificador CVE-2019-7667 para esta vulnerabilidad.
- Autenticación inadecuada: la aplicación permitiría realizar una autenticación de manera inadecuada utilizando el valor de *hash* MD5 de la contraseña, lo que podría permitir a un atacante con acceso a la base de datos iniciar sesión sin la necesidad de descifrar la contraseña. Se ha asignado el identificador CVE-2019-7666 para esta vulnerabilidad.
- Uso de credenciales embebidas: la versión *flash* de la interfaz web posee un usuario y contraseña embebidos, lo que posibilitaría a un atacante autenticado realizar una escalada de privilegios. Se ha asignado el identificador CVE-2019-7672 para esta vulnerabilidad.

Para el resto de vulnerabilidades, se han asignado los identificadores CVE-2019-7280, CVE-2019-7281 y CVE-2019-7671.

Etiquetas: Actualización, Vulnerabilidad