Boletín de octubre de 2020

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en productos Bosch

Fecha de publicación: 01/10/2020

Importancia: Alta

Recursos afectados:

- Bosch PRAESENSA, versiones 1.10 y anteriores;
- Bosch PRAESIDEO, versiones 4.41 y anteriores.

Descripción:

Bosch ha publicado 3 vulnerabilidades, 2 de severidad alta y una media, en sus productos PRAESIDEO Network Controller y en PRAESENSA System Controller que podrían permitir a un atacante realizar acciones arbitrarias o llevar a cabo ataques del tipo Cross-Site-Scripting (XSS) almacenado.

Solución:

- Actualizar a PRAESIDEO versión 4.42 y PRAESENSA versión 1.20.
- Los controladores LBB4401/00 y PRS-NCO-B Network Controllers no pueden ser actualizados a PRAESIDEO 4.42, por lo que se recomienda aislar la red de la red pública. Si esto no fuera posible, se recomienda utilizar un *firewall*.

Detalle:

- Una vulnerabilidad en la interfaz de gestión basada en la web de Bosch PRAESIDEO y Bosch PRAESENSA podría permitir que un atacante remoto, no autenticado, realice acciones arbitrarias en un sistema en nombre de otro usuario (Cross-Site Request Forgery). Esto requiere que la víctima sea engañada para que haga clic en un enlace malicioso o envíe un formulario malicioso. Se ha asignado el identificador CVE-2020-6776 para esta vulnerabilidad de severidad alta.
- El servidor web GoAhead utilizado en Bosch PRAESIDEO no protege adecuadamente contra los ataques de repetición de intentos en la autenticación de HTTP Digest. Se ha asignado el identificador CVE-2020-15688 para esta vulnerabilidad de severidad alta.
- Una vulnerabilidad en la interfaz de gestión basada en la web de Bosch PRAESIDEO y Bosch PRAESENSA podría permitir que un atacante remoto autenticado, con privilegios de administrador, realice un ataque *Cross-Site-Scripting* (XSS) almacenado contra otro usuario. Cuando la víctima se conecta a la interfaz de gestión, el código almacenado se ejecuta en el contexto de su navegador. Se ha asignado el identificador CVE-2020-6777 para esta vulnerabilidad de severidad media.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en varios productos de WAGO

Fecha de publicación: 01/10/2020

Importancia: Crítica

Recursos afectados:

Versiones de *firmware* 07 y anteriores de los siguientes productos:

- 750-852;

- 750-880/xxx-xxx;
- 750-881;
- 750-831/xxx-xxx;
- 750-882;
- 750-885/xxx-xxx;
- 750-889.

Versiones de *firmware* 03 y anteriores de los siguientes productos:

- 750-362;
- 750-363;
- 750-823;
- 750-832/xxx-xxx;
- 750-862;
- 750-891;
- 750-890/xxx-xxx.

Versiones de *firmware* 13 y anteriores de los siguientes productos:

- 750-352;
- 750-831/xxx-xxx;
- 750-852;
- 750-880/xxx-xxx;
- 750-881;
- 750-889.

Descripción:

Los investigadores Maxim Rupp y Secuninja, ambos coordinados por el , han identificado 3 vulnerabilidades, con severidades crítica, alta y media, en distintos productos de WAGO que han reportado al propio fabricante.

Solución:

Actualizar a versiones de *firmware* superiores a 07 los siguientes productos:

- 750-852;
- 750-880/xxx-xxx;
- 750-881;
- 750-831/xxx-xxx;
- 750-882;
- 750-885/xxx-xxx;
- 750-889.

Actualizar a versiones de *firmware* superiores a 03 los siguientes productos:

- 750-362;
- 750-363;
- 750-823;
- 750-832/xxx-xxx;
- 750-862;
- 750-891;
- 750-890/xxx-xxx.

Actualizar a versiones de *firmware* 14 o superiores los siguientes productos:

- 750-352;
- 750-831/xxx-xxx;
- 750-852;
- 750-880/xxx-xxx;
- 750-881;
- 750-889.

Detalle:

- Esta vulnerabilidad permitiría a un atacante, que tuviese acceso al WBM (*Web-Based Management*), evitar la carga de la aplicación en tiempo de ejecución, después de reiniciar el dispositivo mediante el envío de solicitudes diseñadas específicamente sin autenticación. Se ha asignado el identificador CVE-2020-12505 para esta vulnerabilidad.
- Esta vulnerabilidad permitiría a un atacante, que tuviese acceso al WBM y conocimiento sobre su estructura de directorios, cambiar la configuración de parámetros de los dispositivos enviando solicitudes diseñadas específicamente sin autenticación, lo que podría provocar un mal funcionamiento de la aplicación después de reiniciar. Se ha asignado el identificador CVE-2020-12506 para esta vulnerabilidad.
- La página de configuración SNMP del dispositivo es vulnerable a un ataque XSS persistente. Un atacante necesitaría un inicio de sesión autorizado en el dispositivo para vulnerar la web de configuración de SNMP con *scripts* maliciosos, lo que podría utilizarse para instalar código malicioso y obtener acceso a información confidencial. Se ha asignado el identificador CVE-2018-16210 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Omisión de autenticación en IBM Maximo Asset Management

Fecha de publicación: 02/10/2020

Importancia: Crítica

Recursos afectados:

- IBM Maximo Asset Management, versiones 7.6.0 y 7.6.1.
- Productos de soluciones industriales afectados en caso de utilizar una versión core afectada:
  - Maximo para aviación;
  - Maximo para ciencias;
  - Maximo para energía nuclear;
  - Maximo para petróleo y gas;
  - Maximo para transporte;
  - Maximo para utilidades.
- Productos IBM Control Desk afectados en caso de utilizar una versión core afectada:
  - SmartCloud Control Desk;
  - IBM Control Desk;
  - Tivoli Integration Composer.

Descripción:

IBM ha publicado una vulnerabilidad de severidad crítica que podría permitir a un atacante la omisión de autenticación.

Solución:

Aplicar el Interim Fix o el Fix Pack correspondiente al producto afectado:

- Para la versión 7.6.1.2:
  - aplicar Maximo Asset Management 7.6.1.2 Feature Pack 7.6.1.2-TIV-MAMMT-FP002 o el último Interim Fix disponible.
- Para la versión 7.6.1.1:
  - aplicar Maximo Asset Management 7.6.1.1 iFix 7.6.1.1-TIV-MBS-IFIX002 o el último Interim Fix disponible.
- Para la versión 7.6.1.0:
  - aplicar Maximo Asset Management 7.6.1.0 iFix 7.6.1.0-TIV-MBS-IFIX012 o el último Interim Fix disponible.
- Para la versión 7.6.1.10:
  - aplicar Maximo Asset Management 7.6.0.10 iFix 7.6.0.10-TIV-MBS-IFIX003 o el último Interim Fix disponible.

Detalle:

Por medio de un comando HTTP especialmente diseñado, un atacante podría omitir la autenticación y ejecutar comandos. Se ha asignado el identificador CVE-2020-4493 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en PEPPERL FUCHS Comtrol RocketLinux

Fecha de publicación: 08/10/2020

Importancia: Crítica

Recursos afectados:

P F Comtrol RocketLinx, versiones:

- ES7510-XT,
- ES8509-XT,
- ES8510-XT,
- ES9528-XTv2,
- ES7506,
- ES7510,
- ES7528,
- ES8508,
- ES8508F,
- ES8510,
- ES8510-XTE,
- ES9528/ES9528-XT.

Descripción:

El investigador T. Weber de SEC Consult Vulnerability Lab, coordinado por el , ha identificado múltiples vulnerabilidades en PEPPERL FUCHS Comtrol RocketLinux que ha reportado al propio fabricante.

Solución:

Actualmente el fabricante no ha publicado actualizaciones para solucionar estas vulnerabilidades, por lo que se requieren medidas de protección externas:

- Un *firewall* debe bloquear el tráfico de redes que no son de confianza al dispositivo, especialmente el tráfico dirigido a la página web de administración.
- El acceso de administrador y usuario debe estar protegido por una contraseña segura y solo debe estar disponible para un grupo muy limitado de personas.

Detalle:

Los atacantes remotos podrían explotar múltiples vulnerabilidades para obtener acceso al dispositivo, ejecutar cualquier programa y obtener información.

- Se ha asignado el identificador CVE-2020-12500 para esta vulnerabilidad crítica de tipo autorización incorrecta.
- Se ha asignado el identificador CVE-2020-12501 para esta vulnerabilidad crítica de tipo credenciales embebidas en el *software*.
- Se ha asignado el identificador CVE-2020-12502 para esta vulnerabilidad alta de tipo CSRF (*Cross-Site Request Forgery*).
- Se ha asignado el identificador CVE-2020-12503 para esta vulnerabilidad alta de tipo validación incorrecta de entrada.
- Se ha asignado el identificador CVE-2020-12504 para esta vulnerabilidad crítica de tipo funcionalidad oculta.

Etiquetas: Comunicaciones, IoT, Vulnerabilidad

Autorización incorrecta en American Dynamics victor Web Client de Johnson Controls

Fecha de publicación: 09/10/2020

Importancia: Alta

Recursos afectados:

American Dynamics victor Web Client, todas las versiones hasta la 5.4.1 inclusive.

Descripción:

Joachim Kerschbaumer reportó al fabricante Johnson Controls una vulnerabilidad, con severidad alta, de tipo autorización incorrecta.

Solución:

Actualizar el producto afectado a la versión 5.6.

Detalle:

American Dynamics victor Web Client no realiza una verificación de autorización cuando un atacante, con acceso desde una red adyacente, intenta eliminar archivos arbitrarios del sistema. Se ha asignado el identificador CVE-2020-9048 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Consumo incontrolado de recursos en Mitsubishi Electric MELSEC iQ-R Series

Fecha de publicación: 09/10/2020

Importancia: Alta

Recursos afectados:

Se encuentran afectados los siguientes módulos de MELSEC iQ-R:

- R00 / 01 / 02CPU, todas las versiones,
- CPU R04 / 08/16/32/120 (EN), todas las versiones,
- R08 / 16/32 / 120SFCPU, todas las versiones,
- R08 / 16/32 / 120PCPU, todas las versiones,
- R16 / 32 / 64MTCPU, todas las versiones.

Descripción:

El investigador Yossi Reuven, de SCADAfence, ha identificado una vulnerabilidad en la serie MELSEC iQ-R de Mitsubishi Electric, que podría provocar una denegación de servicio debido al consumo descontrolado de recursos.

Solución:

Mitsubishi Electric publicará un parche próximamente para esta vulnerabilidad. Si tiene preguntas, consulte con un representante de Mitsubishi Electric.

La recomendación de Mitsubishi Electric a los usuarios es que tomen las siguientes medidas de mitigación para minimizar el riesgo:

- Utilice una red privada virtual (VPN) para evitar el acceso no autorizado a través de Internet.
- Minimice la exposición del dispositivo, restrinja el acceso a la red LAN y bloquee el acceso a equipos que no sean de confianza a través de los cortafuegos.

Detalle:

La vulnerabilidad encontrada puede ser explotada de forma remota enviando paquetes, especialmente diseñados, a módulos de la serie MELSEC iQ-R, causando un consumo descontrolado de recursos y una denegación de servicio.

Se ha asignado el identificador CVE-2020-16850 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, SCADA, Vulnerabilidad

Avisos de seguridad de Siemens de octubre de 2020

Fecha de publicación: 09/10/2020

Importancia: Alta

Recursos afectados:

- Desigo Insight, todas las versiones;
- SIPORT MP, versiones anteriores a 3.2.1.

Descripción:

Siemens ha publicado en su comunicado mensual varias actualizaciones de seguridad de diferentes productos.

Solución:

- Actualizar Desigo Insight a la versión 6.0 SP5 y aplicar el *hotfix* 2 o posteriores;
- actualizar SIPORT MP a la versión 3.2.1.

Detalle:

Siemens, en su comunicación mensual de parches de seguridad, ha emitido un total de 9 avisos de seguridad, de los cuales 7 son actualizaciones de avisos publicados anteriormente.

Los tipos de nuevas vulnerabilidades publicadas se corresponden con los siguientes:

- 1 vulnerabilidad de inyección SQL;
- 1 vulnerabilidad de restricción inadecuada de capas o marcos de IU renderizados;
- 1 vulnerabilidad de exposición de información confidencial a un usuario no autorizado;
- 1 vulnerabilidad de uso de la autenticación del lado del cliente.

Para estas vulnerabilidades se han asignado los siguientes identificadores: CVE-2020-15792, CVE-2020-15793, CVE-2020-15794 y CVE-2020-7591.

Etiquetas: Actualización, Infraestructuras críticas, Siemens, Vulnerabilidad

---

Múltiples vulnerabilidades en ARC Informatique PcVue

Fecha de publicación: 13/10/2020

Importancia: Crítica

Recursos afectados:

ARC Informatique PcVue, versiones desde 8.10 hasta la anterior a 12.0.17.

Descripción:

Sergey Temnikov y Andrey Muravitsky, investigadores de Kaspersky ICS CERT, han descubierto 3 vulnerabilidades, 1 con severidad crítica y 2 altas, de tipo ejecución remota de código, denegación de servicio y exposición de información, que afectan a ARC Informatique PcVue.

Solución:

El proveedor proporcionará información detallada para solucionar estas vulnerabilidades en el boletín de seguridad SB2020-1 (se requiere inicio de sesión) disponible en el listado de Alertas de Seguridad de PcVue.

Detalle:

- Debido a la deserialización insegura de los mensajes recibidos en la interfaz, se puede realizar una ejecución de código arbitrario (RCE) en el servidor *backend* de *Web & Mobile*. Se ha asignado el identificador CVE-2020-26867 para esta vulnerabilidad.
- Debido a la capacidad de un usuario no autorizado de modificar la información utilizada para validar los mensajes enviados por clientes web legítimos, una vulnerabilidad de denegación de servicio (DoS) podría evitar que los usuarios legítimos se conecten y operen correctamente con WebVue, WebScheduler o la aplicación móvil TouchVue. Se ha asignado el identificador CVE-2020-26868 para esta vulnerabilidad.
- Una vulnerabilidad de exposición de información podría permitir a un usuario no autorizado acceder a los datos de sesión de usuarios legítimos a través de WebVue, WebScheduler o la aplicación móvil TouchVue. Se ha asignado el identificador CVE-2020-26869 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, IoT, SCADA, Vulnerabilidad

---

Vulnerabilidad de ruta de búsqueda no confiable en Flexera InstallShield

Fecha de publicación: 14/10/2020

Importancia: Alta

Recursos afectados:

- Flexera InstallShield, versiones hasta la 2015 SP1;
- Flexera InstallShield está integrado en muchos productos vendidos por otras empresas.

Descripción:

Un investigador anónimo ha notificado al fabricante una vulnerabilidad, de severidad alta, de tipo ruta de búsqueda no confiable.

Solución:

Se recomienda que los usuarios se comuniquen con el equipo de soporte del proveedor del producto para obtener orientación sobre las mitigaciones y soluciones alternativas a esta vulnerabilidad. Para más información, consultar el artículo KBR de Flexera.

Detalle:

El producto afectado está expuesto a una vulnerabilidad de ruta de búsqueda no confiable, que podría permitir a un atacante ejecutar un DLL malicioso si se situase en el directorio de trabajo del archivo ejecutable del programa de instalación, a través de métodos de ingeniería social. Se ha asignado el identificador CVE-2016-2542 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Microsoft, Vulnerabilidad, Windows

---

Múltiples vulnerabilidades en MOXA NPort IAW5000A-I/O Series

Fecha de publicación: 14/10/2020

Importancia: Crítica

Recursos afectados:

NPort IAW5000A-I/O con versión de *firmware* 2.1 o anterior.

Descripción:

Evgeniy Druzhinin y Ilya Karpov de Rostelecom-Solar han descubierto seis vulnerabilidades en MOXA NPort IAW5000A-I/O Series que podrían permitir a un atacante remoto acceder a información confidencial, obtener acceso y secuestro de sesiones, permitir que un usuario realice peticiones con privilegios administrativos o el uso de contraseñas débiles.

Solución:

Moxa ha publicado una versión de *firmware* que corrige estas vulnerabilidades.

Detalle:

La vulnerabilidad más crítica encontrada en MOXA NPort IAW5000A-I/O Series, y que podría permitir utilizar contraseñas débiles, se refiere al servicio web que se integra en este producto y que no requiere a los usuarios que utilicen contraseñas seguras. Se ha asignado el identificador CVE-2020-25153 para esta vulnerabilidad.

Otras vulnerabilidades encontradas en MOXA NPort IAW5000A-I/O Series disponen de los siguientes identificadores: CVE-2020-25198, CVE-2020-25194, CVE-2020-25190, CVE-2020-25196 y CVE-2020-25192.

Etiquetas: Actualización, Infraestructuras críticas, SCADA, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Schneider Electric

Fecha de publicación: 14/10/2020

Importancia: Crítica

Recursos afectados:

- M340 CPUs: BMX P34x, versiones de *firmware* anteriores a 3.20.
- Módulos M340 Communication Ethernet:
  - BMX NOE 0100 (H), versiones anteriores a 3.3;
  - BMX NOE 0110 (H), versiones anteriores a 6.5;

    - BMX NOC 0401, versiones anteriores a 2.10.
- Procesadores *premium* con Ethernet COPRO integrado: TSXP574634, TSXP575634 y TSXP576634, versiones anteriores a 6.1.
- Módulos de comunicación *premium*:
    - TSXETY4103, versiones anteriores a 6.2;
    - TSXETY5103, versiones anteriores a 6.4.
- Procesadores *quantum* con Ethernet COPRO integrado: 140CPU65xxxxx, versiones anteriores a 6.1.
- Módulos de comunicación *quantum*:
    - 140NOE771x1, versiones anteriores a 7.1;
    - 140NOC78x00, versiones anteriores a 1.74;
    - 140NOC77101, versiones anteriores a 1.08.
- Todas las versiones de los productos:
    - EcoStruxure Machine Expert (anteriormente conocido como SoMachine y SoMachine Motion);
    - E PLC400;
    - E PLC100;
    - E PLC_Setup;
    - EcoStruxure Machine SCADA Expert.
- Acti9:
    - Smartlink SI D, todas las versiones anteriores a 002.004.002;
    - Smartlink SI B, todas las versiones anteriores a 002.004.002;
    - PowerTag Link / Link HD, todas las versiones anteriores a 001.008.007;
    - Smartlink EL B, todas las versiones anteriores a 1.2.1.
- Wiser:
    - Link, todas las versiones anteriores a 1.5.0;
    - Energy, todas las versiones anteriores a 1.5.0.
- EcoStruxure™:
    - Power Monitoring Expert, versiones 9.0, 8.x y 7.x;
    - Energy Expert, versión 2.0:
    - Power SCADA Operation con Advanced Reporting y Dashboards Module, versión 9.0.
- Power Manager, versiones 1.1, 1.2 y 1.3.
- StruxureWare™ PowerSCADA Expert con Advanced Reporting y Dashboards Module, versiones 8.x.

Descripción:

Schneider Electric ha publicado múltiples vulnerabilidades, 2 críticas, 7 altas y 2 medias, de tipo gestión de credenciales, corrupción de memoria, longitud de campos no verificada, creación de archivos de licencia arbitrarios, comunicación remota con la API de CodeMeter, alteración o creación de archivo de licencia, retorno de paquetes con información del *heap*, valores insuficientemente aleatorios, control de acceso inadecuado y neutralización incorrecta de la entrada durante la generación de una página web.

Solución:

Seguir las instrucciones de actualización y configuración descritas en la sección *Remediation* de cada aviso del fabricante.

Detalle:

Las vulnerabilidades de severidad crítica aparecen descritas a continuación:

- Existe una vulnerabilidad de gestión de credenciales que podría provocar la ejecución de comandos en el servidor web sin autenticación, al enviar peticiones HTTP especialmente diseñadas. Se ha asignado el identificador CVE-2020-7533 para esta vulnerabilidad.
- Existe una vulnerabilidad de corrupción de memoria donde el mecanismo del analizador de paquetes de CodeMeter (todas las versiones anteriores a 7.10a) no verifica la longitud de los campos. Un atacante podría enviar paquetes, especialmente diseñados, para explotar esta vulnerabilidad. Se ha asignado el identificador CVE-2020-14509 para esta vulnerabilidad.

Para el resto de vulnerabilidades, se han asignado los siguientes identificadores: CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, CVE-2020-16233, CVE-2020-7548, CVE-2020-7545, CVE-2020-7546 y CVE-2020-7547.

Etiquetas: Actualización, Infraestructuras críticas, SCADA, Schneider Electric, Vulnerabilidad

---

Vulnerabilidad de desbordamiento de búfer en Fieldcomm Group HART-IP y hipserver

Fecha de publicación: 14/10/2020

Importancia: Crítica

Recursos afectados:

- HART-IP Developer kit, versión 1.0.0.0;
- hipserver, versión 3.6.1.

Descripción:

El investigador Reid Wightman, de Dragos, Inc., ha descubierto una vulnerabilidad de desbordamiento de búfer que podría permitir a un atacante bloquear el dispositivo o realizar una ejecución remota de código.

Solución:

Fieldcomm Group recomienda a los usuarios restringir el acceso a los equipos que ejecuten este *software*. Los usuarios de hipserver deben actualizar a la versión 3.7.0 o posterior.

Detalle:

La vulnerabilidad descubierta en Fieldcomm Group HART-IP y hipserver podría utilizarse a través de mensajes HART-IP con cargas útiles lo suficientemente grandes, causando un desbordamiento de búfer basado en la pila y pudiendo bloquear el dispositivo u obtener el control del dispositivo. Se ha asignado el identificador CVE-2020-16209 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Validación de entrada incorrecta en SPRECON-E de Aprecher Automation

Fecha de publicación: 15/10/2020

Importancia: Alta

Recursos afectados:

SPRECON-E, versiones de *firmware* anteriores a 8.64b.

Descripción:

Gregor Bonney, empleado de CyberRange-e en Innogy, ha coordinado la publicación del aviso que notifica una vulnerabilidad, con severidad alta, de tipo validación de entrada incorrecta del archivo de configuración en SPRECON-E.

Solución:

Actualizar SPRECON-E a la versión de *firmware* 8.64b. Además, el fabricante ofrece una versión actualizada del *firmware*, actualmente 8.64d, para los clientes a través de sus asesores.

Detalle:

El *firmware* Sprecher SPRECON-E anterior a 8.64b podría permitir a un atacante local insertar código arbitrario. Este *firmware* carece de la validación de los valores de entrada en el lado del dispositivo, que es proporcionada por el software de ingeniería durante la parametrización. Por lo tanto, un atacante con acceso a archivos de configuración locales podría insertar comandos maliciosos para que se ejecutasen después de compilarlos en archivos de parámetros válidos ("PDL"), transferirlos al dispositivo y reiniciarlo. Se ha asignado el identificador CVE-2020-11496 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en varios productos de Advantech

Fecha de publicación: 16/10/2020

Importancia: Alta

Recursos afectados:

- WebAccess/SCADA, versiones 9.0 y anteriores;
- R-SeeNet, versiones desde 1.5.1 hasta 2.4.10.

Descripción:

Los investigadores Sivathmican Sivakumaran de ZDI de Trend Micro, y el conocido como *rgod*, en colaboración con ZDI de Trend Micro, han reportado 2 vulnerabilidades, ambas con severidad alta, de tipo control externo de nombre de archivo o ruta e inyección SQL.

Solución:

- Actualizar WebAccess/SCADA a la versión 9.0.1 o posteriores;
- actualizar R-SeeNet a la versión 2.4.11 o posteriores.

Detalle:

- El componente WADashboard de WebAccess/SCADA podría permitir a un atacante controlar o influir en una ruta utilizada en una operación en el sistema de archivos, otorgándole la posibilidad de ejecutar código de forma remota como administrador. Se ha asignado el identificador CVE-2020-25161 para esta vulnerabilidad.
- La página web de R-SeeNet es vulnerable a una inyección SQL, que podría permitir a un atacante remoto invocar consultas en la base de datos y obtener información confidencial. Se ha asignado el identificador CVE-2020-25157 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, SCADA, Vulnerabilidad

---

Vulnerabilidad de identificación inadecuada en

múltiples productos de la serie COMTRAXX de Bender

Fecha de publicación: 19/10/2020

Importancia: Alta

Recursos afectados:

Todos los dispositivos que ejecutan el software COMTRAXX están afectados por esta vulnerabilidad. Concretamente, las versiones anteriores a 4.2.0 de los siguientes productos:

- COM465IP, número de orden B95061065 y B95061066;
- COM465DP, número de orden B95061060 y B95061061;
- COM465ID, número de orden B95061070;
- CP700, número de orden B95061030;
- CP907, número de orden B95061080;
- CP915, número de orden B95061081, B95061085 y B95061092.

Descripción:

El investigador, Maxim Rupp, coordinado por el , ha identificado una vulnerabilidad, de tipo identificación inadecuada, en distintos productos de la serie COMTRAXX de Bender, que ha reportado al propio fabricante.

Solución:

Actualizar a la versión 4.2.0.

Detalle:

La autorización del usuario está validada para la mayoría de las rutas del sistema, pero no para todas. Un atacante que posea conocimientos sobre las rutas podría leer y escribir datos de configuración sin autorización previa, omitiendo de esta manera la verificación de credenciales. Se ha asignado el identificador CVE-2019-19885 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Autenticación inadecuada en XMC20 Multiservice-Multiplexer de Hitachi ABB Power Grids

Fecha de publicación: 21/10/2020

Importancia: Crítica

Recursos afectados:

- XMC20 R4 utilizando COGE5, versiones anteriores a co5ne_r1h07_12.esw;
- XMC20 R6 utilizando COGE5, versiones anteriores a co5ne_r2d14_03.esw.

Descripción:

Hitachi ABB Power Grids ha reportado una vulnerabilidad, con severidad crítica, de tipo autenticación inadecuada.

Solución:

- XMC20 R4: actualizar a la versión COGE5 co5ne_r1h07_12.esw o posteriores;
- XMC20 R6: actualizar a la versión COGE5 co5ne_r2d14_03.esw o posteriores.

Detalle:

Un atacante podría aprovechar la vulnerabilidad descrita, que se encuentra en una librería utilizada por los productos afectados, enviando un mensaje especialmente diseñado al nodo XMC20 para abrir un canal de comunicación sin realizar primero la autenticación, lo que provocaría un acceso no autorizado. Se ha asignado el identificador CVE-2018-10933 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Desbordamiento de búfer en 1794-AENT Flex I/O Series B de Rockwell Automation

Fecha de publicación: 21/10/2020

Importancia: Alta

Recursos afectados:

El adaptador Ethernet/IP 1794-AENT Flex I/O Series B, versión 1794-AENT Flex I/O, Series B, 4.003 y anteriores.

Descripción:

El investigador, Jared Rittle, de Cisco Talos, ha reportado esta vulnerabilidad, de severidad alta, a Rockwell Automation que podría permitir la ejecución remota de código.

Solución:

Rockwell Automation recomienda el uso de controles de seguridad y una adecuada segmentación de red.

Detalle:

Vulnerabilidades de desbordamiento del búfer en Ethernet/IP Request Path Port Segment, Ethernet/IP Request Path Logical Segment y Ethernet/IP Request Path Data Segment, podrían permitir a un atacante remoto, no autenticado, enviar un paquete malicioso que provoque una condición de denegación de servicio en el dispositivo. Se han asignado los identificadores CVE-2020-6083, CVE-2020-6084 y CVE-2020-6086 para estas vulnerabilidades.

Etiquetas: Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en múltiples productos de B. Braun Melsungen

Fecha de publicación: 23/10/2020

Importancia: Alta

Recursos afectados:

- OnlineSuite AP, versión 3.0 y anteriores;
- SpaceCom, versiones de *software* U61 y anteriores (en Estados Unidos), y L81 y anteriores (fuera de Estados Unidos);
- Battery Pack SP con Wi-Fi, versiones de *software* U61 y anteriores (en Estados Unidos), y L81 y anteriores (fuera de Estados Unidos);
- Data module compactplus, versiones de *software* A10 y A11 (no se distribuyen en Estados Unidos).

Descripción:

Múltiples investigadores de diversas entidades, en el contexto de colaboración en el proyecto BSI ManiMed, han reportado 14 vulnerabilidades, 6 con severidad alta, 7 medias y 1 baja, de tipos limitación inadecuada de una ruta de acceso relativa a un directorio restringido (*relative path transversal*), elemento de la ruta de búsqueda no controlada, inyección en macros de Excel, XSS, redirección abierta, inyección en XPath, fijación de sesión, uso de un *hash* unidireccional sin *salt*, verificación inadecuada de firma criptográfica, gestión incorrecta de privilegios, uso de contraseñas embebidas, código para *debugear* aún activo y control de acceso inadecuado.

Solución:

El fabricante recomienda actualizar a las siguientes versiones, para solucionar las vulnerabilidades descritas:

- OnlineSuite Field Service Information, versión AIS06/20;
- SpaceCom, versiones U62 o posteriores (en Estados Unidos), y L82 o posteriores (fuera de Estados Unidos);
- Battery Pack SP con Wi-Fi, versiones U62 o posteriores (en Estados Unidos), y L82 o posteriores (fuera de Estados Unidos);
- Data module compactplus, versión A12 o posteriores.

Detalle:

- Una vulnerabilidad de limitación inadecuada de una ruta de acceso relativa a un directorio restringido (*relative path transversal*) podría permitir a un atacante, no autenticado, cargar y descargar archivos arbitrarios. Se ha asignado el identificador CVE-2020-25172 para esta vulnerabilidad.
- Una vulnerabilidad de secuestro (*hijacking*) de DLL permitiría a un atacante local ejecutar código en el sistema como un usuario con privilegios elevados. Se ha asignado el identificador CVE-2020-25174 para esta vulnerabilidad.
- Una vulnerabilidad de XSS reflejado podría permitir a un atacante remoto inyectar código web arbitrario o HTML en varias ubicaciones. Se ha asignado el identificador CVE-2020-25158 para esta vulnerabilidad.
- Una vulnerabilidad de inyección XPath permitiría a un atacante remoto, no autorizado, acceder a información sensible y escalar privilegios. Se ha asignado el identificador CVE-2020-25162 para esta vulnerabilidad.
- Una vulnerabilidad de limitación inadecuada de una ruta de acceso relativa a un directorio restringido (*relative path transversal*) podría permitir a un atacante con privilegios de usuario del servicio cargar archivos arbitrarios mediante un archivo *.tar* especialmente diseñado. Se ha asignado el identificador CVE-2020-25150 para esta vulnerabilidad.
- El código de depuración activo permitiría a un atacante, en posesión de material criptográfico, acceder al dispositivo como *root*. Se ha asignado el identificador CVE-2020-25156 para esta vulnerabilidad.

Para el resto de vulnerabilidades con severidad media y baja, se han asignado los identificadores: CVE-2020-25170, CVE-2020-25154, CVE-2020-25152, CVE-2020-25164, CVE-2020-25166, CVE-2020-16238, CVE-2020-25168 y CVE-2020-25160.

Etiquetas: Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

---

Múltiples vulnerabilidades en JUUKO Industrial Radio Remote Control de SHUN HU Technology

Fecha de publicación: 28/10/2020

Importancia: Alta

Recursos afectados:

JUUKO Industrial Radio Remote Control K-800 y K-808 con versiones de *firmware* anteriores a los números que terminan en: 9A, 9B, 9C, etc. En caso de duda, consultar el soporte técnico de SHUN HU Technology.

Descripción:

Marco Balduzzi, Philippe Z Lin, Federico Maggi, Jonathan Andersson, Akira Urano, Stephen Hilt y Rainer Vosseler, en colaboración con ZDI de Trend Micro, han reportado 2 vulnerabilidades, ambas de severidad alta, de tipo omisión de autenticación por captura/reproducción e inyección de comandos.

Solución:

SHUN HU Technology ha publicado nuevas versiones de *firmware* que mitigan estas vulnerabilidades, y recomienda a los usuarios que se comuniquen con un representante de ventas o con el soporte técnico para obtener ayuda con estas actualizaciones.

Detalle:

- K-800 es vulnerable a un ataque de reproducción y falsificación de comandos (*authentication bypass by capture-replay*), lo que podría permitir a un atacante reproducir comandos, controlar el dispositivo, ver comandos o hacer que el dispositivo deje de funcionar. Se ha asignado el identificador CVE-2018-17932 para esta vulnerabilidad.
- Un atacante podría crear un paquete, especialmente diseñado, para codificar un comando arbitrario y que podría ejecutarse en el K-808. Se ha asignado el identificador CVE-2018-19025 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad de denegación de servicio en varias familias PLC de WAGO

Fecha de publicación: 28/10/2020

Importancia: Alta

Recursos afectados:

- 750-352,
- 750-831/xxx-xxx,
- 750-852,
- 750-880/xxx-xxx,
- 750-881,
- 750-889.

Las versiones de firmware, desde la FW1, hasta la FW10 están afectadas. Todas las versiones nuevas desde la FW11, lanzada en diciembre de 2017, no se ven afectadas.

Descripción:

El investigador, William Knowles (Applied Risk), ha reportado a WAGO una vulnerabilidad, coordinada por el , que podría permitir a un atacante la denegación del servicio.

Solución:

Actualizar el dispositivo a la última versión de firmware.

Detalle:

Un atacante podría bloquear el dispositivo mediante el envío de una serie de paquetes, especialmente diseñados, a los puertos HTTP (S) 80/443. Se ha asignado el identificador CVE-2020-12516 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en varios productos de Mitsubishi Electric

Fecha de publicación: 30/10/2020

Importancia: Crítica

Recursos afectados:

Las siguientes versiones de MELSEC iQ-R Series están afectadas:

- R 00/01/02 CPU, versiones de *firmware* 20 y anteriores;
- R 04/08/16/32/120 (EN) CPU, versiones de *firmware* 52 y anteriores;
- R 08/16/32/120 SFCPU, versiones de *firmware* 22 y anteriores;
- R 08/16/32/120 PCPU, todas las versiones;

- R 08/16/32/120 PSFCPU, todas las versiones;
- R 16/32/64 MTCPU, todas las versiones.

Los siguientes módulos de MELSEC iQ-R Series están afectados:

- EtherNet/IP Network Interface Module, RJ71EIP91: si los primeros 2 dígitos del número de serie son 02 o anteriores;
- PROFINET IO Controller Module, RJ71PN92: si los primeros 2 dígitos del número de serie son 01 o anteriores;
- High Speed Data Logger Module, RD81DL96: si los primeros 2 dígitos del número de serie son 08 o anteriores;
- MES Interface Module, RD81MES96N: si los primeros 2 dígitos del número de serie son 04 o anteriores;
- OPC UA Server Module, RD81OPC96: si los primeros 2 dígitos del número de serie son 04 o anteriores.

Las siguientes versiones de MELSEC Q Series están afectadas:

- Q03 UDECPU, Q 04/06/10/13/20/26/50/100 UDEHCPU, número de serie 22081 y anteriores;
- Q 03/04/06/13/26 UDVCPU, número de serie 22031 y anteriores;
- Q 04/06/13/26 UDPVCPU, número de serie 22031 y anteriores;
- Q 172/173 DCPU hasta Q 172/173 DCPU-S1, todas las versiones;
- Q 172/173 DSCPU, todas las versiones;
- Q 170 MCPU, todas las versiones;
- Q 170 MSCPU hasta Q 170 MSCPU (-S1), todas las versiones;
- MR-MQ100, todas las versiones.

Las siguientes versiones de MELSEC L Series están afectadas:

- L 02/06/26 CPU (-P), L 26 CPU - (P) BT, todas las versiones.

Descripción:

Mitsubishi Electric ha reportado 7 vulnerabilidades, 2 con severidad crítica, 4 altas y 1 media, de tipos restricción incorrecta de operaciones dentro de los límites de un búfer de memoria, control de acceso inadecuado, fijación de sesión, desreferencia a puntero nulo, inyección de argumento, consumo descontrolado de recursos y errores de gestión de recursos.

Solución:

Consultar la sección de *Countermeasures* de los dos avisos oficiales del fabricante (2020-012_en y 2020-013_en) para aplicar las actualizaciones adecuadas.

Detalle:

Las vulnerabilidades con severidad crítica podrían permitir que un atacante remoto, no autenticado, detuviese las funciones de red de los productos o ejecutase un programa malicioso a través de un paquete especialmente diseñado. Se han asignado los identificadores CVE-2020-5653 y CVE-2020-5656 para estas vulnerabilidades.

Para el resto de vulnerabilidades, se han asignado los identificadores: CVE-2020-5654, CVE-2020-5655, CVE-2020-5657, CVE-2020-5652 y CVE-2020-5658.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad