Boletín de noviembre de 2020

Avisos de Sistemas de Control Industrial

Múltiples vulnerabilidades en NEXCOM NIO 50

Fecha de publicación: 04/11/2020

Importancia: Media

Recursos afectados:

NEXCOM NIO 50, todas las versiones.

Descripción:

Zero Day Initiative ha reportados 2 vulnerabilidades, ambas de severidad media, de tipo validación incorrecta de datos de entrada y transmisión en texto claro de información sensible.

Solución:

NEXCOM ya no vende ni mantiene NIO 50 y lo considera un producto al final de su vida útil.

Detalle:

- El producto afectado no valida correctamente la entrada, lo que podría permitir que un atacante ejecutase un ataque de denegación de servicio (DoS). Se ha asignado el identificador CVE-2020-25151 para esta vulnerabilidad.
- El producto afectado transmite información confidencial no cifrada, lo que podría permitir que un atacante accediese a esta información. Se ha asignado el identificador CVE-2020-25155 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en MXview Series de Moxa

Fecha de publicación: 05/11/2020

Importancia: Crítica

Recursos afectados:

MXview Series, versiones de *firmware* desde la 3.0, hasta la 3.1.8.

Descripción:

Yuri Kramarz, de Cisco Talos, ha reportado a Moxa múltiples vulnerabilidades de severidad crítica, del tipo permisos incorrectos por defecto.

Solución:

Descargar el nuevo *software*, seguir el procedimiento de copia de seguridad y migración para actualizar MXview.

Si tiene problemas durante este proceso, puede ponerse en contacto con el soporte técnico de Moxa.

Detalle:

Un atacante podría editar un archivo fuente para insertar código especialmente diseñado y conseguir la escalada de

privilegios. Se han asignado los identificadores CVE-2020-13536 y CVE-2020-13537 para estas vulnerabilidades.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Desbordamiento de búfer en PLC Editor de WECON

Fecha de publicación: 06/11/2020

Importancia: Alta

Recursos afectados:

- PLC Editor, versiones 1.3.8 y anteriores.

Descripción:

Natnael Samson y Francis Provencher, junto con Trend Micro's Zero Day Initiative, han reportado estas vulnerabilidades, de severidad alta, al CISA.

Solución:

WECON está desarrollando una solución, para más información puede contactar con WECON desde el portal web .

Detalle:

- Una vulnerabilidad de desbordamiento de búfer basado en pila (stack) podría permitir a un atacante la ejecución arbitraria de código. Se ha asignado el identificador CVE-2020-25177 para esta vulnerabilidad.
- Una vulnerabilidad de desbordamiento de búfer en la región heap de la memoria podría permitir a un atacante la ejecución arbitraria de código. Se ha asignado el identificador CVE-2020-25181 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en Mitsubishi Electric GT14 de las series GOT1000

Fecha de publicación: 06/11/2020

Importancia: Crítica

Recursos afectados:

Los siguientes modelos de GOT1000 con CoreOS, versión 05.65.00.BD y anteriores, se ven afectados:

- GT1455-QTBDE,
- GT1450-QMBDE,
- GT1450-QLBDE,
- GT1455HS-QTBDE,
- GT1450HS-QMBDE.

Descripción:

Mitsubishi Electric ha reportado 6 vulnerabilidades al CISA, 2 con severidad crítica, 3 altas y 1 media, de tipo 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 y errores de gestión de recursos.

Solución:

Siguiendo los pasos descritos en el aviso *2020-014_en* del fabricante, actualizar Core OS a la versión 05.76.00.BG y posteriores (MELSOFT GT Designer3 Version1 [GOT1000], versión 1.245F y posteriores).

Detalle:

Las vulnerabilidades de severidad crítica se describen a continuación:

- El producto afectado tiene una vulnerabilidad de corrupción de memoria, que podría permitir que un atacante enviase un paquete, especialmente diseñado, que podría resultar en una condición de denegación de servicio (DoS) o ejecución de código. Se ha asignado el identificador CVE-2020-5644 para esta vulnerabilidad.
- El producto afectado tiene un problema de control de acceso, que podría permitir que un atacante enviase un paquete, especialmente diseñado, que podría resultar en una condición de denegación de servicio (DoS) o ejecución de código. Se ha asignado el identificador CVE-2020-5647 para esta vulnerabilidad.

Para el resto de vulnerabilidades, se han asignado los siguientes identificadores: CVE-2020-5645, CVE-2020-5646, CVE-2020-5648 y CVE-2020-5649.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en Visual Components de KUKA

Fecha de publicación: 09/11/2020

Importancia: Alta

Recursos afectados:

Visual Components Network License Server, versión 2.0.8.

Descripción:

Sharon Brizinov, investigador de seguridad de Claroty, ha descubierto 2 vulnerabilidades, ambas de severidad alta, de tipo exposición de información confidencial a un usuario no autorizado y excepción no detectada.

Solución:

Para la vulnerabilidad con identificador CVE-2020-10292 se recomienda, como medida de mitigación, no iniciar Visual Components mientras esté conectado a LAN o WAN y contener la simulación a través de la virtualización. Para la otra vulnerabilidad no se aportan medidas de mitigación.

Detalle:

- El protocolo filtra información sobre la información del servidor receptor, la información de la licencia y la gestión de licencias, entre otros. A través de esta vulnerabilidad, un atacante podría recuperar información sobre un sistema de simulación de KUKA, particularmente, la versión del servidor de licencias, que está conectado al simulador, y que le permitiría lanzar simulaciones locales con características similares, entendiendo mejor la dinámica de la virtualización del movimiento y abriendo la posibilidad a realizar otros ataques. Se ha asignado el identificador CVE-2020-10291 para esta vulnerabilidad.
- El protocolo es vulnerable a una condición de denegación de servicio (DoS) a través de una derivación de puntero arbitraria. Esta vulnerabilidad podría permitir que un atacante pasase un paquete especialmente diseñado que, cuando fuese procesado por el servicio, hiciese que un puntero arbitrario de la pila fuese desreferenciado, provocando una excepción no detectada que finalizase el servicio. Se ha asignado el identificador CVE-2020-10292 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, Virtualización, Vulnerabilidad

---

Vulnerabilidad en Oracle WebLogic Server afecta a Sistemas de Control Industrial

Fecha de publicación: 10/11/2020

Importancia: Crítica

Recursos afectados:

Algunos fabricantes utilizan Oracle WebLogic Server en sus productos y soluciones, por lo que se ven afectados.

- Productos de Philips:
  - Tasy EMR v12.2.1.3.

Descripción:

Esta vulnerabilidad, facilmente explotable, podría permitir que un atacante no autenticado, con acceso a la red a través de HTTP, comprometa Oracle WebLogic Server, utilizado en Sistemas de Control Industrial. Este aviso ya fue publicado en INCIBE-CERT como Vulnerabilidad de ejecución remota de código en Oracle WebLogic Server.

Solución:

Seguir las instrucciones descritas en el documento de disponibilidad de parches *Fusion Middleware* (requiere *login*).

Detalle:

Esta vulnerabilidad, relacionada con CVE-2020-14882, ya abordada en las actualizaciones críticas en Oracle (octubre 2020), podría permitir que un atacante no autenticado, con acceso a la red a través de HTTP, comprometa Oracle WebLogic Server. Se puede explotar de forma remota y sin la necesidad de un nombre de usuario, ni contraseña. Se ha asignado el identificador CVE-2020-14750 para esta vulnerabilidad.

Etiquetas: Actualización, Java, Oracle, Sanidad, Vulnerabilidad

---

Avisos de seguridad de Siemens de noviembre de 2020

Fecha de publicación: 10/11/2020

Importancia: Crítica

Recursos afectados:

- SCALANCE W1750D, todas las versiones;
- familia SIMATIC S7-300 CPU (incluyendo las CPU ET200 relacionadas y las variantes SIPLUS), todas las versiones;
- SINUMERIK 840D sl, todas las versiones.

Descripción:

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

Solución:

- Actualizar SCALANCE W1750D a la última versión de *firmware* disponible y seguir las instrucciones descritas en *Control Plane Security Best Practices*; según la configuración de la red y la tolerancia al riesgo, es posible que no se requiera ninguna acción.
- Proteger el acceso a la red por el puerto 102/tcp de la familia SIMATIC S7-300 CPU y SINUMERIK 840D sl.

Detalle:

Siemens, en su comunicación mensual de parches de seguridad, ha emitido un total de 6 avisos de seguridad, de los cuales 4 son actualizaciones de avisos publicados anteriormente.

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

- 1 vulnerabilidad de validación de entrada incorrecta;
- 1 vulnerabilidad de consumo descontrolado de recursos.

Para estas vulnerabilidades se han asignado los siguientes identificadores: CVE-2016-2031 y CVE-2020-15783.

Etiquetas: Actualización, Infraestructuras críticas, Siemens, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Schneider Electric

Fecha de publicación: 11/11/2020

Importancia: Crítica

Recursos afectados:

- M340 CPUs:
  - BMX P34x, todas las versiones.
- Módulos M340 Communication Ethernet:
  - BMX NOE 0100 (H), todas las versiones;
  - BMX NOE 0110 (H), todas las versiones;
  - BMX NOC 0401, todas las versiones;
  - BMX NOR 0200H, todas las versiones.
- Procesadores *premium* con Ethernet COPRO integrado:
  - TSXP574634, TSXP575634 y TSXP576634, todas las versiones.
- Módulos de comunicación *premium:*
  - TSXETY4103, todas las versiones;
  - TSXETY5103, todas las versiones.
- Procesadores *quantum* con Ethernet COPRO integrado:
  - 140CPU65xxxxx, todas las versiones.
- Módulos de comunicación *quantum*:
  - 140NOE771x1, todas las versiones;
  - 140NOC78x00, todas las versiones;
  - 140NOC77101, todas las versiones.
- EcoStruxure™ Operator Terminal Expert Runtime 3.1 Service Pack 1A y anteriores instalados en:
  - Windows PC usando BIOS en modo *legacy*;
  - Harmony iPC (HMIG5U, HMIG5U2) usando BIOS en modo *legacy*.
- IGSS Definition (Def.exe), versión 14.0.0.20247 y anteriores.
- EcoStruxure Building Operation:
  - WebReports, versiones desde 1.9, hasta 3.1;
  - WebStation, versiones desde 2.0, hasta 3.1;
  - instalador Enterprise Server, versiones desde 1.9, hasta 3.1;
  - instalador Enterprise Central, versiones desde 2.0, hasta 3.1.
- Modicon M221, todas las referencias en todas las versiones.
- Easergy T300, versión de *firmware* 2.7 y anteriores.
- PLC Simulator para EcoStruxure™ Control Expert, todas las versiones.
- PLC Simulator para Unity Pro (llamado anteriormente EcoStruxure™ Control Expert), todas las versiones.

Descripción:

Schneider Electric ha publicado múltiples vulnerabilidades, 3 con severidad crítica, 16 altas, 9 medias y 2 bajas.

Solución:

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

Detalle:

Las vulnerabilidades de severidad crítica aparecen descritas a continuación:

- Existe una vulnerabilidad, de tipo control de acceso inadecuado, que podría causar una amplia gama de problemas, entre los que se encuentran exposición de información, denegación de servicio (DoS) y ejecución de comandos cuando el acceso a un recurso de un atacante no está restringido o lo está incorrectamente. Se ha asignado el identificador CVE-2020-7561 para esta vulnerabilidad.
- Existe una vulnerabilidad, de tipo desbordamiento de búfer clásico, que podría causar un bloqueo del simulador de PLC presente en el software EcoStruxure™ Control Expert al recibir una solicitud, especialmente diseñada, a través de Modbus. Se ha asignado el identificador CVE-2020-7559 para esta vulnerabilidad.
- Existe una vulnerabilidad, de tipo restricción inadecuada de intentos excesivos de autenticación, que podría causar la ejecución de comandos no autorizados cuando se realiza un ataque de fuerza bruta a través de Modbus. Se ha asignado el identificador CVE-2020-28212 para esta vulnerabilidad.

Para el resto de vulnerabilidades, se han asignado los siguientes identificadores: CVE-2020-7562, CVE-2020-7563, CVE-2020-7564, CVE-2020-7544, CVE-2020-7550, CVE-2020-7551, CVE-2020-7552, CVE-2020-7553, CVE-2020-7554, CVE-2020-7555, CVE-2020-7556, CVE-2020-7557, CVE-2020-7558, CVE-2020-7569, CVE-2020-7570, CVE-2020-7571, CVE-2020-7572, CVE-2020-28209, CVE-2020-28210, CVE-2020-7565, CVE-2020-7566, CVE-2020-7567, CVE-2020-7568, CVE-2020-7538, CVE-2020-28211 y CVE-2020-28213.

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

---

Múltiples vulnerabilidades en productos OSIsoft

Fecha de publicación: 11/11/2020

Importancia: Alta

Recursos afectados:

- Versiones anteriores a PI Interface para OPC XML-DA 1.7.3.x.
- Versiones anteriores a PI Vision 2020.

Descripción:

Se han identificado dos vulnerabilidades de severidad alta y una de severidad media que afectan a productos de OSIsoft. Un atacante podría aprovechar estas vulnerabilidades para realizar una inyección de código arbitrario o relevar información no autorizada.

Solución:

Actualizar a la última versión los productos afectados:

- PI Interface para OPC XML-DA 1.7.3.x.
- PI Vision 2020 3.5.0.

Detalle:

Se ha descubierto una vulnerabilidad de severidad alta que afecta al producto PI Interface para OPC XML-DA y que podría permitir a un atacante ejecutar código arbitrario de forma remota al controlar un servidor OPC XML-DA. Se ha asignado el identificador CVE-2013-0006 para esta vulnerabilidad.

Otra de las vulnerabilidades de severidad alta afecta al producto PI Vision y podría permitir a un atacante, con acceso de escritura a archivos de PI ProcessBook, inyectar código de forma remota, el cual se importa a PI Vision. Se ha asignado el identificador CVE-2020-25163 para esta vulnerabilidad.

Para la vulnerabilidad de severidad media se ha asignado el identificador CVE-2020-25167.

Etiquetas: Actualización, Vulnerabilidad

Consumo de recursos no controlado en Mitsubishi Electric MELSEC iQ-R series

Fecha de publicación: 13/11/2020

Importancia: Media

Recursos afectados:

Mitsubishi Electric informa que la vulnerabilidad afecta a los siguientes productos de módulos de CPU de la serie MELSEC iQ-R:

- R00/01/02 CPU, versiones de *firmware* desde 05, hasta 19;
- R04/08/16/32/120(EN) CPU, versiones de *firmware* desde 35, hasta 51.

Descripción:

El investigador chino, Xiaofei.Zhang, ha reportado una vulnerabilidad, con severidad media, de tipo consumo de recursos no controlado.

Solución:

El fabricante recomienda actualizar a las siguientes versiones de *firmware* para solucionar esta vulnerabilidad:

- R00/01/02 CPU, versiones de *firmware* 20 o posteriores;
- R04/08/16/32/120(EN) CPU, versiones de *firmware* 52 o posteriores.

Detalle:

Existe una vulnerabilidad de denegación de servicio (DoS) debido al consumo incontrolado de recursos en los módulos de CPU de la serie MELSEC iQ-R. Esta vulnerabilidad no afecta a los productos cuando el parámetro *To Use or Not to Use Web Server* de los módulos de la CPU se configura en *Not Use*, que es la configuración predeterminada. Se ha asignado el identificador CVE-2020-5666 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Autenticación inadecuada en productos Becton, Dickinson and Company (BD)

Fecha de publicación: 13/11/2020

Importancia: Alta

Recursos afectados:

- BD Alaris PC Unit, Model 8015, versiones 9.33.1 y anteriores;
- BD Alaris Systems Manager, versiones 4.33 y anteriores.

Descripción:

Medigate ha reportado a BD esta vulnerabilidad de severidad alta, del tipo autenticación inadecuada, que podría permitir a un atacante la denegación del servicio.

Solución:

BD ha proporcionado las siguientes mitigaciones:

- Como parte de las actualizaciones normales del servidor de BD, muchas de las instalaciones de Systems Manager ya se han actualizado a una versión que soluciona esta vulnerabilidad.
- BD planea lanzar una próxima versión del software BD Alaris PC Unit para las versiones 12.0.1, 12.0.2, 12.1.0 y 12.1.2 de BD Alaris Systems Manager.
- Habilitar el firewall en el servidor de Systems Manager e implementar reglas sobre las restricciones de puertos y servicios, según el documento técnico de seguridad del producto de BD.

Para obtener información adicional, consulte el boletín de seguridad del producto BD.

Detalle:

Una vulnerabilidad de autenticación inadecuada de sesión de red, dentro del proceso de autenticación entre versiones específicas de BD Alaris PC Unit y BD Alaris Systems Manager, podría permitir a un atacante la denegación de servicio en la unidad de PC BD Alaris, modificando los encabezados de configuración de los datos en tránsito. Esto provocaría una caída en la capacidad inalámbrica de la unidad de PC BD Alaris, lo que supondría el funcionamiento manual de la unidad de PC. Se ha asignado el identificador CVE-2020-25165 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

---

Múltiples vulnerabilidades en Paradox IP150

Fecha de publicación: 18/11/2020

Importancia: Crítica

Recursos afectados:

Paradox IP150, versión de *firmware* 5.02.09.

Descripción:

Omri Ben-Bassat, investigador de Microsoft, ha notificado 2 vulnerabilidades, 1 de severidad crítica y 1 alta, de tipo desbordamiento de búfer basado en pila (*stack*) y desbordamiento de búfer clásico.

Solución:

Contactar con el soporte de Paradox, para obtener detalles de las medidas de mitigación, por correo electrónico a través de **.

Detalle:

- El producto afectado es vulnerable a 3 desbordamientos de búfer basados en pila (*stack*), lo que podría permitir que un atacante, no autenticado, ejecutase código arbitrario de forma remota. Se ha asignado el identificador CVE-2020-25189 para esta vulnerabilidad de severidad crítica.
- El producto afectado es vulnerable a 5 desbordamientos de búfer posteriores a la autenticación (conocido como

desbordamiento de búfer clásico), que podrían permitir que un usuario que haya iniciado sesión ejecute código arbitrario de forma remota. Se ha asignado el identificador CVE-2020-25185 para esta vulnerabilidad de severidad alta.

Etiquetas: Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Verificación de autorización inadecuada en victor Web Client de Johnson Controls

Fecha de publicación: 18/11/2020

Importancia: Alta

Recursos afectados:

- Victor Web Client, versión 5.6 y anteriores;
- C ? CURE Web Client, versión 2.90 y anteriores.

El nuevo cliente C ? CURE 9000 basado en web, que se introdujo en C ? CURE 9000 v2.90, no se ve afectado

Descripción:

Joachim Kerschbaumer ha reportado una vulnerabilidad, del tipo autenticación inadecuada, a Johnson Controls, Inc.

Solución:

Actualizar a:

- victor Unified Client v5.6 SP1;
- Web Client_c2.70_5.2_Update02;
- Web Client_c2.80_v5.4.1_Update04;
- CCureWeb_2.90_Update01.

Detalle:

Una vulnerabilidad de verificación de autorización inadecuada podría permitir a un atacante no autenticado, en la red, crear y firmar su propio token web JSON y usarlo para ejecutar un método de API HTTP sin la necesidad de una autenticación/autorización válida. En determinadas circunstancias, esto podría afectar a la disponibilidad del sistema mediante la realización de un ataque de denegación de servicio. Se ha asignado el identificador CVE-2020-9049 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad de desbordamiento de búfer en EtherNet/IP de Real Time Automation (RTA)

Fecha de publicación: 18/11/2020

Importancia: Crítica

Recursos afectados:

Versiones anteriores a 2.28 de 499ES EtherNet/IP Adaptor Source Code, en su pila TCP/IP.

Descripción:

Sharon Brizinov, investigador de Claroty, ha descubierto una vulnerabilidad de desbordamiento de búfer en la región *stack* de la memoria, lo que permitiría a un atacante remoto provocar una denegación de servicio, o la ejecución remota de código en el dispositivo afectado.

Solución:

Se recomienda contactar con el servicio de soporte de Real Time Automation.

Adicionalmente, se recomienda las siguientes medidas de mitigación:

- Minimice la exposición de la red para todos los dispositivos.
- Ubique los sistemas de control industrial detrás de firewalls y aíslelos de la red empresarial o de gestión.
- Cuando se requiera acceso remoto, utilice métodos seguros, como redes privadas virtuales (VPN).

Detalle:

La vulnerabilidad encontrada en EtherNet/IP de Real Time Automation podría permitir un desbordamiento de búfer en la región *stack* de la memoria a través del envío de un paquete, especialmente diseñado, que podría causar denegación de servicio (DoS) o ejecución de código (RCE).

Se ha asignado el identificador CVE-2020-25159 para esta vulnerabilidad.

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

Vulnerabilidad de escalada de privilegios en TwinCAT System Tray de Beckhoff

Fecha de publicación: 20/11/2020

Importancia: Alta

Recursos afectados:

TwinCAT XAR, versiones 3.1 con una ruta de instalación por defecto.

Descripción:

El investigador, Ayushman Dutta, ha informado a de una vulnerabilidad en las instalaciones por defecto de TwinCAT XAR, en concreto en la ruta de instalación y los permisos de TwinCAT System Tray, a través del ejecutable TcSysUI.exe. Debido a esta vulnerabilidad, un usuario local podría reemplazar o modificar los ejecutables que otros usuarios del mismo sistema podrían ejecutar, produciéndose una escalada de privilegios en el mismo.

Solución:

Se recomienda realizar la instalación de TwinCAT en la ruta 'C:/Program Files/TwinCAT' o 'C:/Archivos de programa/TwinCAT'.

En caso de tener ya el programa instalado en otra ruta, se recomienda desinstalarlo e instalarlo nuevamente en la ruta correcta indicada. Utilice la instalación personalizada para ello. Se recomienda realizar una copia de seguridad del dispositivo completo antes de dicha acción, y eliminar luego los archivos en otras rutas.

Detalle:

La vulnerabilidad encontrada podría permitir a un usuario del sistema realizar modificaciones en los archivos y programas usados en la ruta de instalación por defecto "C:/TwinCAT" de TwinCAT, incluyendo el programa TcSysUI.exe que se carga por defecto al arranque del sistema para TwinCat System Tray. Esto incluye a usuarios administradores, por lo que si un usuario sin privilegios administrativos modifica esos ficheros, podría realizar una elevación de privilegios en el sistema al iniciar sesión un administrador.

Se ha asignado el identificador CVE-2020-12510 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, IoT, Vulnerabilidad, Windows

Múliples vulnerabilidades en varios productos de Endress Hauser

Fecha de publicación: 20/11/2020

Importancia: Crítica

Recursos afectados:

- Para la vulnerabilidad CVE-2020-12495:
  - Ecograph T: versiones de *firmware* igual o superiores a 1.0.0 (07/2013);
  - Ecograph T Neutral/Private Label; versiones de *firmware* anteriores a 2.0.0 (08/2015).
- Para la vulnerabilidad CVE-2020-12496, versiones de *firmware* igual o superiores a 2.0.0 (08/2015) en los siguientes productos:
  - Ecograph T,
  - Memograph M,
  - Ecograph T Neutral/Private Label,
  - Memograph M Neutral/Private Label.

Descripción:

El investigador, Maxim Rupp, ha reportado al fabricante Endress Hauser 2 vulnerabilidades, de tipos gestión de privilegios inadecuada y exposición de información confidencial a un usuario no autorizado, que afectan a varios dispositivos. El fabricante, a su vez, ha notificado esta vulnerabilidad al

Solución:

El fabricante recomienda que los clientes configuren un *firewall* perimetral para bloquear el tráfico de redes y usuarios que no sean de confianza para el dispositivo. Estas recomendaciones se incorporarán a la documentación del dispositivo (instrucciones de funcionamiento). Además, se debe cambiar la contraseña predeterminada para la cuenta de operador, servicio y administrador.

Detalle:

- El dispositivo afectado tiene una interfaz web de usuario con un sistema de acceso, basado en *tokens* dinámicos, que tiene asignados roles con diferentes privilegios de escritura y lectura. La vulnerabilidad consiste en que las sesiones de usuario no se cierran correctamente, y a un usuario con menos privilegios se le asignan los privilegios más elevados cuando inicia sesión. Se ha asignado el identificador CVE-2020-12495 para esta vulnerabilidad de severidad crítica.
- La versión de *firmware* tiene un *token* dinámico para cada solicitud enviada al servidor, lo que hace que las solicitudes repetidas y el análisis sean lo suficientemente complejos. Sin embargo, se detectó un problema con la matriz de control de acceso en el lado del servidor, que posibilitaría a un usuario con pocos privilegios la obtención de información de los *endpoints* a los que no debería tener acceso en condiciones normales. Se ha asignado el identificador CVE-2020-12496

para esta vulnerabilidad de severidad media.

Etiquetas: Infraestructuras críticas, Sanidad, Vulnerabilidad

Consumo de recursos no controlado en Mitsubishi Electric MELSEC iQ-R series

Fecha de publicación: 20/11/2020

Importancia: Alta

Recursos afectados:

Mitsubishi Electric informa que la vulnerabilidad afecta a los siguientes productos de módulos de CPU de la serie MELSEC iQ-R:

- R00/01/02 CPU, versiones de *firmware* 19 y anteriores;
- R04/08/16/32/120 (EN) CPU, versiones de *firmware* 51 y anteriores;
- R08/1632/120 SFCPU, versiones de *firmware* 22 y anteriores;
- R08/16/32/120 PCPU, todas las versiones;
- R08/16/32/120 PSFCPU, todas las versiones;
- RJ71EN71, versiones de *firmware* 47 y anteriores;
- RJ71GF11-T2, versiones de *firmware* 47 y anteriores;
- RJ72GF15-T2, versiones de *firmware* 07 y anteriores;
- RJ71GP21-SX, versiones de *firmware* 47 y anteriores;
- RJ71GP21S-SX, versiones de *firmware* 47 y anteriores;
- RJ71C24(-R2/R4), todas las versiones;
- RJ71GN11-T2, todas las versiones.

Descripción:

Xiaofei.Zhang ha descubierto una vulnerabilidad, de tipo consumo incontrolado de recursos y de severidad alta, que provocaría una denegación de servicio (DoS) en los productos afectados.

Solución:

El fabricante recomienda actualizar a las siguientes versiones de *firmware* para solucionar esta vulnerabilidad:

- R00/01/02 CPU, versiones 20 o posteriores;
- R04/08/16/32/120 (EN) CPU, versiones 52 o posteriores;
- R08/16/32/120 SFCPU, versiones 23 o posteriores;
- RJ71EN71, versiones 48 o posteriores;
- RJ71GF11-T2, versiones 48 o posteriores;
- RJ72GF15-T2, versiones 08 o posteriores;
- RJ71GP21-SX, versiones 48 o posteriores;
- RJ71GP21S-SX, versiones 48 o posteriores.

Detalle:

La vulnerabilidad, de tipo consumo no controlado de recursos, podría suponer una condición de denegación de servicio (DoS) en la ejecución y comunicación de los módulos de CPU de la serie MELSEC iQ-R, después de que el atacante enviase un paquete SLMP, especialmente diseñado. Se ha asignado el identificador CVE-2020-5668 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en FactoryTalk Linx de Rockwell Automation

Fecha de publicación: 25/11/2020

Importancia: Crítica

Recursos afectados:

FactoryTalk Linx, versión 6.11 y anteriores.

Descripción:

Sharon Brizinov, investigador de Claroty, reportó estas 3 vulnerabilidades al Rockwell Automation PSIRT. Las vulnerabilidades tienen unas severidades crítica, alta y media, y son de tipo desbordamiento de búfer basado en *heap* (crítica y media) y validación de entrada inadecuada (alta).

Solución:

Actualizar FactoryTalk Linx a la versión 6.10/6.11 (consultar *Patch Answer ID* 1126433). Adicionalmente, el usuario puede actualizar a 6.20, que está disponible en PCDC (requiere *login*).

Detalle:

- Una vulnerabilidad de desbordamiento de montículo (*heap*) en FactoryTalk Linx, podría permitir que un atacante

remoto, no autenticado, enviar rangos de puertos maliciosos, lo que podría resultar en una ejecución remota de código (RCE). Se ha asignado el identificador CVE-2020-27251 para esta vulnerabilidad crítica.
- Un fallo en la rutina de verificación de Ingress/Egress de FactoryTalk Linx, podría permitir a un atacante remoto, no autenticado, generar un paquete, especialmente diseñado, que resultase en una condición de denegación de servicio (DoS) en el dispositivo. Se ha asignado el identificador CVE-2020-27253 para esta vulnerabilidad alta.
- Una vulnerabilidad de desbordamiento de montículo (*heap*) en FactoryTalk Linx, podría permitir a un atacante remoto, no autenticado, enviar conjuntos de solicitudes de atributos maliciosos, lo que podría resultar en la filtración de información confidencial. A su vez, esta divulgación de información podría conducir a la omisión ASLR (*Address Space layout Randomization*). Se ha asignado el identificador CVE-2020-27255 para esta vulnerabilidad media.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad en Fuji Electric V-Server Lite

Fecha de publicación: 25/11/2020

Importancia: Alta

Recursos afectados:

V-Server Lite, todas las versiones anteriores a 3.3.24.0.

Descripción:

Tran Van Khang-khangkito, de VinCSS, en colaboración con ZDI, ha reportado una vulnerabilidad de tipo escritura fuera de límites.

Solución:

Actualizar el *software* a la versión 3.3.25.0.

Detalle:

El producto afectado es vulnerable a la escritura fuera de los límites de memoria, lo que podría permitir a un atacante ejecutar código arbitrario de forma remota. Se ha asignado el identificador CVE- 2020-25171 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad