Boletín de febrero de 2021

Avisos de Sistemas de Control Industrial

Desbordamiento de búfer en Rockwell Automation MicroLogix 1400

Fecha de publicación: 03/02/2021

Importancia: Alta

Recursos afectados:

MicroLogix 1400, versión 21.6 y anteriores de todas sus series.

Descripción:

El Instituto Tecnológico Veermata Jijabai ha reportado a Rockwell Automation una vulnerabilidad, de severidad alta, de tipo desbordamiento de búfer, que podría originar una condición de denegación de servicio (DoS).

Solución:

Rockwell Automation recomienda mitigar el riesgo y aplicar las directrices generales de seguridad para una estrategia global de defensa en profundidad. Para ellos, todos los usuarios deben desactivar, si es posible, el soporte de Modbus TCP, cuando no sea necesario para la implementación de MicroLogix 1400. Sin Modbus TCP habilitado, un potencial atacante no tiene acceso para explotar el dispositivo utilizando esta vulnerabilidad.

Para más medidas de mitigación, consultar la sección *4. MITIGATIONS* del aviso del CISA.

Detalle:

Un atacante remoto, no autenticado, podría enviar un paquete Modbus, especialmente diseñado, permitiéndole recuperar o modificar valores aleatorios en el registro. La explotación exitosa podría provocar un desbordamiento de búfer que resultaría en una condición de denegación de servicio (DoS). El LED de FALLO parpadeará en ROJO y las comunicaciones podrían perderse. La recuperación de la condición de DoS requiere que el usuario subsane el fallo. Se ha asignado el identificador CVE-2021-22659 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, SCADA, Vulnerabilidad

Vulnerabilidad de denegación de servicio en AC500 V2 de ABB

Fecha de publicación: 03/02/2021

Importancia: Alta

Recursos afectados:

Los siguientes productos AC500 V2, con interfaz *ethernet* integrada, están afectados por esta vulnerabilidad:

- PM554,
- PM556,
- PM564,
- PM566,
- PM572,

- PM573.

Descripción:

Richard Thomas y Tom Chothia, de la Universidad de Birmingham, han reportado a ABB una vulnerabilidad en AC500 V2, de severidad alta, que podría permitir a un atacante causar una condición de denegación de servicio (DoS).

Solución:

Actualmente no hay ninguna solución disponible.

Para evitar la explotación de esta vulnerabilidad, todos los productos afectados deberán utilizarse únicamente como se describe en '*Manual for PLC Automation with AC500 V2 and Automation Builder 2.4.0*', concretamente en el capítulo '*Cyber security in AC500 V2 products*', especialmente en lo que respecta a la defensa en profundidad y al funcionamiento seguro.

Detalle:

La vulnerabilidad puede ser explotada para hacer que el componente de visualización web del PLC se detenga y no responda, lo que provocaría que los usuarios perdiesen la visibilidad remota del estado del PLC. Si un usuario intentase iniciar sesión en el PLC, mientras se explota esta vulnerabilidad, el PLC mostrará un estado de error y rechazará las conexiones a Automation Builder. Se ha asignado el identificador CVE-2020-24686 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Infraestructuras críticas, SCADA, Vulnerabilidad

---

Denegación de servicio en Flex IO 1794-AENT/B de Allen-Bradley

Fecha de publicación: 03/02/2021

Importancia: Alta

Recursos afectados:

Flex IO 1794-AENT/B, versión 4.003.

Descripción:

El investigador, Jared Rittle, de Cisco Talos, ha informado de una vulnerabilidad de severidad alta que podría permitir a un atacante causar una condición de denegación de servicio (DoS).

Solución:

Actualmente, no existe ninguna actualización disponible.

Detalle:

Una vulnerabilidad de desbordamiento de búfer, en la funcionalidad del segmento de red de la ruta de solicitud ENIP, podría permitir a un atacante la denegación del servicio mediante el envío de una solicitud de red especialmente diseñada. Se ha asignado el identificador CVE- 2020-6088 para esta vulnerabilidad.

Etiquetas: 0day, Actualización, Comunicaciones, Vulnerabilidad

---

Vulnerabilidad de lectura fuera de límites en Cscape de Horner Automation

Fecha de publicación: 05/02/2021

Importancia: Alta

Recursos afectados:

Cscape, todas las versiones anteriores a 9.90 SP3.5.

Descripción:

Francis Provencher {PRL}, en colaboración con ZDI de Trend Micro, ha notificado una vulnerabilidad, de severidad alta, de lectura fuera de límites en el producto Cscape de Horner Automation.

Solución:

Horner Automation recomienda a los usuarios actualizar Cscape a la versión 9.90 SP3.5.

Detalle:

Cscape carece de una validación adecuada de los datos suministrados por el usuario al analizar los archivos del proyecto, lo que podría llevar a una vulnerabilidad de lectura fuera de límites. Un atacante podría aprovechar esta vulnerabilidad para ejecutar código en el contexto del proceso actual. Se ha asignado el identificador CVE-2021-22663 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en KeyShot de Luxion

Fecha de publicación: 05/02/2021

Importancia: Alta

Recursos afectados:

- KeyShot, versiones anteriores a la 10.1;
- KeyShot Viewer, versiones anteriores a la 10.1;
- KeyShot Network Rendering, versiones anteriores a la 10.1;
- KeyVR, versiones anteriores a la 10.1.

Descripción:

rgod, trabajando conjuntamente con Trend Micro's Zero Day Initiative, ha reportado múltiples vulnerabilidades que podrían permitir a un atacante la ejecución de código arbitrario, el almacenamiento de *scripts* arbitrarios en las carpetas de inicio automático y el ataque a los productos sin la suficiente advertencia de la interfaz de usuario.

Solución:

Actualizar a KeyShot (v10.1).

Detalle:

- La escritura fuera de límites al procesar archivos de proyecto, podría permitir a un atacante ejecutar código arbitrario. Se ha asignado el identificador CVE-2021-22647 para esta vulnerabilidad.
- La lectura fuera de límites al procesar archivos de proyecto, podría permitir a un atacante ejecutar código arbitrario. Se ha asignado el identificador CVE-2021-22643 para esta vulnerabilidad.
- Los documentos .bip muestran un comando "load", que puede apuntar a un .dll desde un recurso compartido de red remoto. Esto hace que el .dll pueda ser ejecutado sin la suficiente advertencia de la UI. Se ha asignado el identificador CVE-2021-22645 para esta vulnerabilidad.
- Múltiples problemas de desreferencia de puntero NULL al procesar archivos de proyecto, podrían permitir a un atacante ejecutar código arbitrario. Se ha asignado el identificador CVE-2021-22649 para esta vulnerabilidad.
- Una vulnerabilidad de salto de directorios podría permitir a un atacante almacenar *scripts* arbitrarios en las carpetas de inicio automático, mediante la carga de un archivo especialmente diseñado. Se ha asignado el identificador CVE-2021-22651 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

Vulnerabilidades en GE Digital iFIX

Fecha de publicación: 08/02/2021

Importancia: Alta

Recursos afectados:

GE Digital HMI/SCADA iFIX v6.1 y anteriores.

Descripción:

Sharon Brizinov, de Claroty, y William Knowles, junto con Applied Risk, han informado a GE Digital de 3 vulnerabilidades que podrían permitir a un atacante modificar la configuración de GE Digital iFIX de todo el sistema del usuario.

Solución:

Actualizar a GE Digital's iFIX v6.5.

Detalle:

Las vulnerabilidades podrían permitir a un atacante con acceso a una sesión autenticada modificar la configuración de GE Digital iFIX en todo el sistema del usuario.

Etiquetas: Actualización, Infraestructuras críticas, SCADA, Vulnerabilidad

Avisos de seguridad de Siemens de febrero de 2021

Fecha de publicación: 09/02/2021

Importancia: Crítica

Recursos afectados:

- SINEC NMS, todas las versiones anteriores a la 1.0 SP1 Update 1;

- SINEMA Server, todas las versiones anteriores a la 14.0 SP2 Update 2;
- Nucleus NET, todas las versiones anteriores a la 5.2;
- Nucleus ReadyStart para ARM, MIPS y PPC, todas las versiones anteriores a la 2012.12;
- RUGGEDCOM ROX MX5000, todas las versiones anteriores a la 2.14.0;
- RUGGEDCOM ROX RX1400, todas las versiones anteriores a la 2.14.0;
- RUGGEDCOM ROX RX1500, todas las versiones anteriores a la 2.14.0;
- RUGGEDCOM ROX RX1501, todas las versiones anteriores a la 2.14.0;
- RUGGEDCOM ROX RX1510, todas las versiones anteriores a la 2.14.0;
- RUGGEDCOM ROX RX1511, todas las versiones anteriores a la 2.14.0;
- RUGGEDCOM ROX RX1512, todas las versiones anteriores a la 2.14.0;
- RUGGEDCOM ROX RX5000, todas las versiones anteriores a la 2.14.0;
- PCS neo (Administration Console), versión 3.0;
- TIA Portal, versiones 15, 15.1 y 16;
- DIGSI 4, todas las versiones anteriores a la 4.94 SP1 HF 1;
- JT2Go, todas las versiones anteriores a la 13.1.0.1;
- Teamcenter Visualization, todas las versiones anteriores a la 13.1.0.1;
- familia SCALANCE W780 y W740 (IEEE 802.11n), todas las versiones anteriores a la 6.3;
- configuración de SIMARIS, todas las versiones;
- SIMATIC PCS 7, todas las versiones;
- SIMATIC WinCC, todas las versiones anteriores a la 7.5 SP2.

Descripción:

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

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas pueden obtenerse desde el panel de descarga de Siemens. Para los productos sin actualizaciones disponibles es recomendable aplicar las medidas de mitigación descritas en la sección de *Referencias*.

Detalle:

Siemens, en su comunicación mensual de parches de seguridad, ha emitido un total de 25 avisos de seguridad, de los cuales 16 son actualizaciones.

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

- limitación incorrecta del nombre de la ruta a un directorio restringido (*path traversal*),
- valores insuficientemente aleatorios en los ISN (*Initial Sequence Numbers*) de conexiones TCP,
- validación de entrada incorrecta,
- denegación de servicio,
- verificación insuficiente de autenticidad de los datos,
- validación incorrecta del certificado,
- lectura fuera de límites,
- ejecución de código con privilegios de SYSTEM,
- ejecución de código en el contexto del proceso actual,
- desbordamiento de búfer,
- escritura fuera de límites,
- escalada de privilegios,
- omisión de autenticación.

Para estas vulnerabilidades se han reservado los siguientes identificadores: CVE-2020-25237, CVE-2020-28388, CVE-2018-12404, CVE-2018-18508, CVE-2019-11745, CVE-2019-17006, CVE-2019-17007, CVE-2020-1763, CVE-2020-25238, CVE-2020-25245, CVE-2020-26998, CVE-2020-26999, CVE-2020-27000, CVE-2020-27001, CVE-2020-27002, CVE-2020-27003, CVE-2020-27004, CVE-2020-27005, CVE-2020-27006, CVE-2020-27007, CVE-2020-27008, CVE-2020-28394, CVE-2020-26989, CVE-2020-26990, CVE-2020-26991, CVE-2021-25173, CVE-2021-25174, CVE-2021-25175, CVE-2021-25176, CVE-2021-25177, CVE-2021-25178, CVE-2021-25666, CVE-2020-28392 y CVE-2020-10048.

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

---

Múltiples vulnerabilidades en PowerLogic Power Metering de Schneider Electric

Fecha de publicación: 10/02/2021

Importancia: Alta

Recursos afectados:

- ION7400, todas las versiones anteriores a V3.0.0;
- ION7650, todas las versiones;
- ION7700/73xx, todas las versiones (solo afectado por CVE-2021-22702);
- ION83xx/84xx/85xx/8600, todas las versiones;
- ION8650, todas las versiones anteriores a V 4.31.2;
- ION8800, todas las versiones;
- ION9000, todas las versiones anteriores a V3.0.0;
- PM8000, todas las versiones anteriores a V3.0.0.

Descripción:

Schneider Electric ha informado de tres vulnerabilidades en sus productos de medición eléctrica PowerLogic que podrían permitir la revelación de credenciales de usuario al trasmitirse en claro, o acciones no deseadas en un dispositivo cuando se

utiliza HTTP, lo que podría provocar un comportamiento no deseado del dispositivo.

Solución:

- ION7400, actualizar a la versión V3.0.0;
- ION8650, actualizar a la versión V 4.31.2;
- ION9000, actualizar a la versión V3.0.0;
- PM8000, actualizar a la versión V3.0.0;

Para los siguientes productos no existe un parche que solucione estas vulnerabilidades. Schneider Electric recomienda deshabilitar los servicios de Telnet y de HTTP.

- ION7650,
- ION8800.

En el caso de los siguientes productos, para los que tampoco existe parche, Schneider Electric recomienda además de deshabilitar los servicios Telnet y HTTP, su actualización a productos más modernos al carecer de soporte.

- ION7700/73xx,
- ION83xx/84xx/85xx/8600.

Detalle:

Las vulnerabilidades descubiertas en productos PowerLogic se refieren a una vulnerabilidad de tipo Cross-Site Request Forgery que permite que un usuario realice una acción no deseada en el dispositivo a través de HTTP y dos vulnerabilidades de transmisión de información sensible en texto claro, que podrían causar la divulgación de credenciales de usuario a través de Telnet o a través de HTTP.

Se han asignado los identificadores CVE-2021-22701, CVE-2021-22702 y CVE-2021-22703 a estas vulnerabilidades.

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

---

Múltiples vulnerabilidades en iView de Advantech

Fecha de publicación: 10/02/2021

Importancia: Crítica

Recursos afectados:

iView, todas las versiones anteriores a la 5.7.03.6112.

Descripción:

Los investigadores *Anonymous* y *rgod*, junto con ZDI de Trend Micro, y William Vu de Rapid7, han reportado 3 vulnerabilidades de severidad alta y una de severidad crítica que podrían permitir a un atacante remoto revelar información, realizar una escalada de privilegios, leer datos confidenciales y ejecutar código, respectivamente.

Solución:

Actualizar iView a la versión 5.7.03.6112.

Detalle:

- Debido a una vulnerabilidad de inyección SQL, un atacante no autorizado podría divulgar información o realizar una escalada de privilegios. Se han asignado los identificadores CVE-2021-22654 y CVE-2021-22658 para estas vulnerabilidades de severidad alta, respectivamente.
- Una vulnerabilidad de limitación incorrecta del nombre de la ruta a un directorio restringido (*path traversal*) podría permitir a un atacante leer datos confidenciales. Se ha asignado el identificador CVE-2021-22656 para esta vulnerabilidad de severidad alta.
- La ausencia de autenticación en la configuración de iView podría permitir a un atacante, no autorizado, cambiar la configuración y ejecutar código. Se ha asignado el identificador CVE-2021-22652 para esta vulnerabilidad de severidad crítica.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en la pila TCP/IP implementada en Nut/Net, CycloneTCP, NDKTCPIP, FNET, uC, ulP, picoTCP, MPLAB Net y Nucleus

Fecha de publicación: 12/02/2021

Importancia: Alta

Recursos afectados:

Múltiples productos IoT que utilicen alguna de las siguientes librerías para implementar la pila TCP/IP:

- Nut/Net, versión 5.1 y anteriores;

- CycloneTCP, versión 1.9.6 y anteriores;
- NDKTCPIP, versión 2.25 y anteriores;
- FNET, versión 4.6.3;
- uIP-Contiki-OS (EOL), versión 3.0 y anteriores;
- uC/TCP-IP (EOL), versión 3.6.0 y anteriores;
- uIP-Contiki-NG, versión 4.5 y anteriores;
- uIP (EOL), versión 1.0 y anteriores;
- picoTCP-NG, versión 1.7.0 y anteriores;
- picoTCP (EOL), versión 1.7.0 y anteriores;
- MPLAB Net, versión 3.6.1 y anteriores;
- Nucleus NET, todas las versiones anteriores a 5.2;
- Nucleus ReadyStart para ARM, MIPS y PPC, todas las versiones anteriores a 2012.12.

Descripción:

Daniel dos Santos, Stanislav Dashevskyi, Jos Wetzelsy Amine Amri, investigadores de Forescout Research Labs, informaron del descubrimiento de un total de 9 vulnerabilidades, 8 con severidad alta y 1 media, en las librerías que usan en múltiples dispositivos IoT para la implementación de la pila de comunicaciones TCP/IP.

Todas las vulnerabilidades están relacionadas con el mismo problema: una generación débil del número de secuencia inicial (ISN, *Initial Sequence Number*), que podría utilizarse para secuestrar o falsificar conexiones TCP. En última instancia, los atacantes podrían aprovechar estas vulnerabilidades para cerrar las conexiones en curso, provocando denegaciones de servicio limitadas, para inyectar datos maliciosos en un dispositivo o para saltarse la autenticación.

Solución:

- uIP-Contiki-OS, uIP y picoTCP son productos EOL (*End Of Life*) y no recibirán actualizaciones.
- Nut/Net y uIP-Contiki-NG están desarrollando un parche que publicarán próximamente.
- Los encargados de mantener picoTCP-NG recomiendan a los usuarios actualizar a la versión 2.1 o posteriores.
- Los encargados de mantener MPLAB Net recomiendan a los usuarios actualizar a la versión 3.6.4 o posteriores.
- Siemens recomienda a los usuarios de Nucleus NET actualizar a la última versión de Nucleus ReadyStart, o proteger la información transmitida con protocolos criptográficos como TLS. Se puede encontrar información adicional aquí.
- Siemens recomienda a los usuarios de Nucleus ReadyStart para ARM, MIPS y PPC actualizar a la versión 2012.12 o posteriores, o proteger la información transmitida con protocolos criptográficos como TLS. Se puede encontrar información adicional aquí.
- uC/TCP-IP (EOL). Solucionado en la última versión de Micrium OS (proyecto sucesor).
- Los encargados de mantener CycloneTCP recomiendan a los usuarios actualizar a la versión 2.0.0 o posteriores.
- Texas Instruments recomienda a los usuarios de NDKTCPIP actualizar a la versión 7.02 o posteriores.
- FNET no se actualizará para mitigar esta vulnerabilidad.

Detalle:

- Al predecir el ISN de una conexión TCP existente, los atacantes podrían cerrarla, logrando así una denegación de servicio. O bien, podrían secuestrarla, inyectando datos en una sesión. Los datos pueden inyectarse en el tráfico sensible no cifrado, como las sesiones Telnet (para inyectar comandos), las descargas de archivos FTP (para servir *malware*) o las respuestas HTTP (para dirigir a la víctima a una página maliciosa).

- Al dirigirse a las nuevas conexiones TCP, los atacantes podrían completar con éxito un *handshake* de tres vías y falsificar paquetes de red destinados al *endpoint* de la víctima, o eludir la autenticación basada en direcciones y el control de acceso.

Se han asignado los siguientes identificadores para estas vulnerabilidades: CVE-2020-27213, CVE-2020-27630, CVE-2020-27631, CVE-2020-27632, CVE-2020-27633, CVE-2020-27634, CVE-2020-27635, CVE-2020-27636 y CVE-2020-28388 (este último es el correspondiente a severidad media).

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

---

Ruta de búsqueda no controlada en múltiples productos de Rockwell Automation

Fecha de publicación: 12/02/2021

Importancia: Alta

Recursos afectados:

- DriveTools SP, versiones 5.13 y anteriores;
  - DriveExecutive, versiones 5.13 y anteriores;
- Drives AOP, versiones 4.12 y anteriores.

Descripción:

Las compañías de ciberseguridad industrial, Claroty y Cognite, han reportado a Rockwell Automation una vulnerabilidad, de severidad alta, por la que un atacante podría realizar una escalada de privilegios y así controlar el sistema por completo.

Solución:

Actualizar:

- DriveTools SP a la versión 5.14.41 o una posterior;
- Drives AOP a la versión 4.13.41 o una posterior.

Detalle:

Una vulnerabilidad, de tipo ruta de búsqueda no controlada, presente en ambos productos, podría permitir a un atacante local con privilegios limitados realizar una escalada de privilegios y tomar el control total de los sistemas. Se ha asignado el identificador CVE-2021-22665 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en productos de MB connect line

Fecha de publicación: 16/02/2021

Importancia: Alta

Recursos afectados:

- mymbCONNECT24, versiones 2.6.2 y anteriores;
- mbCONNECT24, versiones 2.6.2 y anteriores.

Descripción:

OTORIO ha comunicado a MB connect line, en coordinación con , 2 vulnerabilidades de severidad baja, 14 vulnerabilidades de severidad media y 2 vulnerabilidades de severidad alta, que podrían permitir a un atacante realizar una escalada de privilegios o acceder a bases de datos.

Solución:

- Para la vulnerabilidad CVE-2020-10384, actualizar a la versión 2.6.2.
- Para la vulnerabilidad CVE-2020-35567, no existe solución por el momento.
- Para la vulnerabilidad CVE-2020-35565, se recomienda activar la detección de fuerza bruta como mitigación, al no disponer de una solución por el momento.
- Para la vulnerabilidad CVE-2020-35561, se recomienda implementar un firewall como mitigación, al no contar una solución por el momento.
- Para el resto de vulnerabilidades, actualizar a la versión 2.7.1.

Detalle:

- Una vulnerabilidad de tipo credenciales embebidas podría permitir a un atacante acceder a una base de datos, ya que la contraseña segura de acceso se comparte entre instancias. Se ha asignado el identificador CVE-2020-35567 para esta vulnerabilidad de severidad alta.
- Una vulnerabilidad de gestión de privilegios inadecuada podría permitir a un atacante realizar una escalada de privilegios local desde la cuenta www-data a la cuenta root. Se ha asignado el identificador CVE-2020-10384 para esta vulnerabilidad de severidad alta.

Para las vulnerabilidades de severidad media se han asignado los identificadores: CVE-2020-35557, CVE-2020-12527, CVE-2020-12528, CVE-2020-35570, CVE-2020-35558, CVE-2020-12529, CVE-2020-35560, CVE-2020-12530, CVE-2020-35564, CVE-2020-35566, CVE-2020-35559, CVE-2020-35568, CVE-2020-35565 y CVE-2020-35561.

Para las vulnerabilidades de severidad baja se han asignado los identificadores: CVE-2020-35563 y CVE-2020-35569.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Múltiples vulnerabilidades en varios productos de PEPPERL FUCHS

Fecha de publicación: 17/02/2021

Importancia: Alta

Recursos afectados:

- PCV/PXV/PGV:
  - versiones 2.0.0 y anteriores de:
    - PGV100-F200A-B17-V1D,
    - PGV150I-F200A-B17-V1D,
    - PGV100-F200-B17-V1D-7477;
  - versiones 4.2.0 y anteriores de:
    - PXV100-F200-B17-V1D,
    - PXV100-F200-B17-V1D-3636;
  - versiones 3.2.3 y anteriores de:
    - PCV80-F200-B17-V1D,
    - PCV100-F200-B17-V1D,
    - PCV50-F200-B17-V1D,
    - PCV100-F200-B17-V1D-6011-6997;
  - versiones 3.2.5 y anteriores de:
    - PCV100-F200-B17-V1D-6011,
    - PCV100-F200-B17-V1D-6011-8203;
  - versiones 1.0.0 y anteriores de:
    - PXV100-F200-B25-V1D,

        - PXV100I-F200-B25-V1D,
        - PCV100-F200-B25-V1D-6011-6720,
        - PCV50-F200-B25-V1D,
        - PCV80-F200-B25-V1D,
        - PCV100-F200-B25-V1D-6011.
- PXV/PGV B28 Profisafe:
    - versiones 1.0.3 y anteriores de:
        - PXV100A-F200-B28-V1D,
        - PXV100A-F200-B28-V1D-6011,
        - PGV100A-F200-B28-V1D,
        - PGV100A-F200A-B28-V1D;
    - versiones 2.1.1 y anteriores de:
        - PGV100AQ-F200A-B28-V1D,
        - PGV100AQ-F200-B28-V1D,
        - PXV100AQ-F200-B28-V1D,
        - PXV100AQ-F200-B28-V1D-6011.
- OHV:
    - versiones 1.1.0 y anteriores de OHV-F230-B17.
- OIT:
    - versiones 1.3.4 y anteriores de OIT500-F113-B17-CB.
- PHA:
    - versiones 3.1.5 y anteriores de:
        - PHA300-F200-B17-V1D,
        - PHA400-F200-B17-V1D,
        - PHA300-F200A-B17-V1D,
        - PHA300-F200-B17-T-V1D,
        - PHA200-F200A-B17-V1D,
        - PHA200-F200-B17-V1D,
        - PHA400-F200A-B17-V1D,
        - PHA300-F200A-B17-T-V1D,
        - PHA600-F200A-B17-V1D,
        - PHA500-F200-B17-V1D,
        - PHA500-F200A-B17-V1D,
        - PHA600-F200-B17-V1D,
        - PHA150-F200A-B17-V1D,
        - PHA200-F200A-B17-T-V1D,
        - PHA150-F200-B17-V1D,
        - PHA800-F200-B17-V1D,
        - PHA400-F200A-B17-T-V1D,
        - PHA500-F200A-B17-T-V1D,
        - PHA700-F200-B17-V1D.
- WCS:
    - versiones 3.0.0 y anteriores de:
        - WCS3B-LS610,
        - WCS3B-LS610H,
        - WCS3B-LS610D,
        - WCS3B-LS610DH,
        - WCS3B-LS610H-OM,
        - WCS3B-LS610DH-OM,
        - WCS3B-LS610D-OM.
        - CS3B-LS610-OM;
    - versiones 1.2.1 y anteriores de:
        - WCS3B-LS510,
        - WCS3B-LS510H,
        - WCS3B-LS510D,
        - WCS3B-LS510DH,
        - WCS3B-LS510H-OM,
        - WCS3B-LS510DH-OM,
        - WCS3B-LS510D-OM,
        - WCS3B-LS510-OM.

Descripción:

El investigador, Hilscher Gesellschaft, de la empresa Systemautomation mbH, ha reportado 2 vulnerabilidades, ambas con severidad alta y que podrían provocar una denegación de servicio, afectando a los componentes PROFINET IO Device y Ethernet IP Stack, usados en múltiples productos de PEPPERL FUCHS. El fabricante, a su vez, ha notificado esta vulnerabilidad al

Solución:

El fabricante no ha publicado ningún parche que solucione estas vulnerabilidades, se recomiendan las siguientes medidas de protección externas:

- minimizar la exposición a la red de los productos afectados y asegurarse de que no son accesibles a través de Internet,
- aislar los productos afectados de la red corporativa,
- utilizar métodos seguros, como las VPN en caso de ser necesario el acceso remoto.

Detalle:

- El componente PROFINET IO Device es vulnerable a un desbordamiento de búfer, que podría permitir a un atacante remoto detener la realización de solicitudes acíclicas, abandonar todas las conexiones cíclicas establecidas o desaparecer completamente de la red. Se ha asignado el identificador CVE-2021-20986 para esta vulnerabilidad.
- El componente Ethernet IP Stack es vulnerable a un desbordamiento de búfer, que podría permitir a un atacante remoto provocar denegación de servicio, ejecución remota de código o exposición de código. Se ha asignado el identificador CVE-2021-20987 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en respiradores Hamilton-T1

Fecha de publicación: 17/02/2021

Importancia: Media

Recursos afectados:

T1 Ventilator, versiones 2.2.3 y anteriores.

Descripción:

Julian Suleder, Raphael Pavlidis y Nils Emmerich, de ERNW Research GmbH, y el Dr. Oliver Matula, de ERNW Enno Rey Netzwerke GmbH, informaron de estas vulnerabilidades a la Oficina Federal de Seguridad de la Información (BSI, Alemania). La BSI proporcionó el informe a CISA. Las vulnerabilidades podrían permitir a un atacante con acceso físico al dispositivo obtener información sensible o provocar una interrupción en el funcionamiento del dispositivo.

Solución:

- Actualizar T1 Ventilator a una versión superior a 2.2.3.

Hamilton Medical recomienda a los usuarios las siguientes medidas preventivas:

- Mantener un control físico estricto del ventilador.
- Estar atento a las notificaciones, alarmas y alertas.
- No conectar el aparato a ningún dispositivo de terceros ni utilizar software no autorizado.

Detalle:

- Las credenciales embebidas en el respirador podrían permitir a los atacantes, con acceso físico al dispositivo, obtener privilegios de administrador para la interfaz de configuración. Se ha asignado el identificador CVE-2020-27278 para esta vulnerabilidad.
- Una vulnerabilidad de validación XML podría permitir a los atacantes, con privilegios y acceso físico, inutilizar el dispositivo de forma persistente mediante la carga de archivos de configuración especialmente diseñados. Se ha asignado el identificador CVE-2020-27282 para esta vulnerabilidad.
- Una vulnerabilidad de divulgación de información podría permitir a los atacantes con acceso físico a los registros de la interfaz de configuración obtener sumas de comprobación válidas para archivos de configuración manipulados. Se ha asignado el identificador CVE-2020-27290 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

Múltiples vulnerabilidades en dispositivos Advantech WebAccess

Fecha de publicación: 17/02/2021

Importancia: Alta

Recursos afectados:

Advantech WebAccess/SCADA versión 9.0.1.

Descripción:

El investigador Yuri Kramarz, de Cisco Talos, ha descubierto varias vulnerabilidades en dispositivos Advantech WebAccess, que permitirían a un atacante realizar una divulgación de información o una escalada de privilegios y ejecución de código con privilegios administrativos en el dispositivo.

Solución:

Advantech WebAccess no ha publicado ningún parche para solucionar estas vulnerabilidades.

Se recomienda reducir el grado de exposición de los dispositivos dentro de su red permitiendo únicamente la conexión desde sistemas confiables. También se recomienda restringir el acceso a los sistemas únicamente a usuarios de confianza.

Detalle:

Las vulnerabilidades encontradas permitirían la divulgación de información a través de una inclusión de archivos locales en la funcionalidad de instalación de Advantech WebAccess, por medio de solicitud HTTP autenticada.

Estas vulnerabilidades también permitirían una elevación de privilegios locales a través de los permisos del sistema de archivos en la instalación de Advantech WebAccess, pudiendo reemplazar módulos binarios o cargados para ejecutar código con privilegios administrativos. Esta vulnerabilidad se produce en diferentes binarios y archivos del sistema, tales como el ejecutable o bibliotecas DLL de PostgreSQL, servicios como *SaaS-Composer_keep-alive*, *WebAccessMongoDB*, *Dashboard* (Grafana) o *WISE-PaaS_SaaS-Composer* entre otros.

Se han asignado los siguientes identificadores para estas vulnerabilidades: CVE-2020-13550, CVE-2020-13551, CVE-2020-13552, CVE-2020-13553, CVE-2020-13554 y CVE-2020-13555

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

---

Denegación de servicio en Allen-Bradley MicroLogix 1100 de Rockwell Automation

Fecha de publicación: 17/02/2021

Importancia: Alta

Recursos afectados:

PLC Allen-Bradley MicroLogix 1100, revisión 1.0.

Descripción:

Cisco Talos ha reportado a Rockwell Automation una vulnerabilidad de severidad alta que podría permitir a un atacante remoto causar una condición de denegación de servicio (DoS).

Solución:

Rockwell Automation recomienda a los usuarios de MicroLogix 1100 que migren a MicroLogix 1400 e instalen el *firmware* de versión 21.006 o posterior.

Para más información, consultar la publicación PN1548.

Detalle:

Una vulnerabilidad debida a la gestión inadecuada del parámetro de longitud de IPv4 para ICMP podría permitir a un atacante, remoto y no autenticado, enviar paquetes especialmente diseñados, lo que resultaría en un *8H Hard Fault* y causaría consecuentemente una condición de denegación de servicio del PLC. Se ha asignado el identificador CVE-2020-6111 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad en Metasys Reporting Engine (MRE) Web Services de Johnson Controls

Fecha de publicación: 19/02/2021

Importancia: Alta

Recursos afectados:

Metasys Reporting Engine (MRE) Web Services, versiones 2.0 y 2.1.

Descripción:

TIM Security Red Team Research informó de una vulnerabilidad, de severidad alta, que podría permitir a un atacante acceder a archivos o directorios que se encuentran fuera del directorio restringido.

Solución:

Actualizar a la versión 2.2 o posterior.

Detalle:

La validación insuficiente de los elementos de la ruta de acceso podría permitir a un atacante resolver una ubicación que está fuera del directorio restringido (*path traversal*). Se ha asignado el identificador CVE-2020-9050 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad de escalada de privilegios en Sytech XL Reporter

Fecha de publicación: 19/02/2021

Importancia: Alta

Recursos afectados:

Sytech XL Reporter versión 14.0.1.

Descripción:

El investigador Yuri Kramarz, de Cisco Talos, ha descubierto una vulnerabilidad en el proceso de instalación de Sytech XL Reporter que permitiría a un atacante una escalada de privilegios local a través de sistema de archivos del directorio de instalación de Sytech XL Reporter. Un atacante también podría sobrescribir los ejecutables del servicio y ejecutar código arbitrario con los privilegios del usuario que ejecuta el servicio.

Solución:

El fabricante no ha publicado ningún parche de seguridad para solucionar esta vulnerabilidad.

Se recomienda no realizar la instalación en la ruta por defecto "C: / XLReporter" y utilizar en su lugar la ruta del sistema "%ProgramFiles%".

Detalle:

El software industrial de visualización y generación de informes con análisis de datos de PLC, HDA, OPC, o históricos Sytech XL Reporter se instala por defecto en una ruta que permite a los usuarios de los grupos "Usuarios autenticados" y el grupo "Todos" tengan privilegios de "Control Total / Modificar" sobre el archivo binario de servicio "XLReporter Runtime", ejecutándose con privilegios NT SYSTEM, lo que permite a los usuarios de ambos grupos leer, escribir o modificar archivos arbitrarios en el directorio de instalación, y llevar a cabo una escalada de privilegios.

Se ha asignado el identificador CVE-2020-13549 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, SCADA, Virtualización

Múltiples vulnerabilidades en múltiples productos de Mitsubishi Electric

Fecha de publicación: 19/02/2021

Importancia: Alta

Recursos afectados:

Los siguientes productos de software de ingeniería FA (*Factory Automation*) que establecen comunicación con los equipos MELSEC, FREQROL o GOT:

- C Controller module setting and monitoring tool, todas las versiones;
- CPU Module Logging Configuration Tool, todas las versiones;
- CW Configurator, todas las versiones;
- Data Transfer, todas las versiones;
- EZSocket, todas las versiones;
- FR Configurator, todas las versiones;
- FR Configurator SW3, todas las versiones;
- FR Configurator2, todas las versiones;
- GT Designer3 Version1(GOT1000), todas las versiones;
- GT Designer3 Version1(GOT2000), todas las versiones;
- GT SoftGOT1000 Version3, todas las versiones;
- GT SoftGOT2000 Version1, todas las versiones;
- GX Configurator-DP, versión 7.14Q y anteriores;
- GX Configurator-QP, todas las versiones;
- GX Developer, todas las versiones;
- GX Explorer, todas las versiones;
- GX IEC Developer, todas las versiones;
- GX LogViewer, todas las versiones;
- GX RemoteService-I, todas las versiones;
- GX Works2, versión 1.597X y anteriores;
- GX Works3, Versión 1.070Y y anteriores;
- M_CommDTM-HART, todas las versiones;
- M_CommDTM-IO-Link, todas las versiones;
- MELFA-Works, todas las versiones;
- MELSEC WinCPU Setting Utility, todas las versiones;
- MELSOFT EM Software Development Kit (EM Configurator), todas las versiones;
- MELSOFT Navigator, todas las versiones;
- MH11 SettingTool Version2, todas las versiones;
- MI Configurator, todas las versiones;
- MT Works2, todas las versiones;
- MX Component, todas las versiones;
- Network Interface Board CC IE Control utility, todas las versiones;
- Network Interface Board CC IE Field Utility, todas las versiones;
- Network Interface Board CC-Link Ver.2 Utility, todas las versiones;
- Network Interface Board MNETH utility, todas las versiones;
- PX Developer, todas las versiones;
- RT ToolBox2, todas las versiones;
- RT ToolBox3, todas las versiones;
- Setting/monitoring tools for the C Controller module, todas las versiones;
- SLMP Data Collector, todas las versiones.

Descripción:

El investigador *dliangfun* ha reportado a Mitsubishi Electric dos vulnerabilidades de severidad alta que podrían permitir a un atacante causar una condición de denegación de servicio.

Solución:

Actualizar a la última versión de cada producto *software*:

- GX Configurator-DP, a la versión 7.15R o posterior;
- GX Works2, a la versión 1.600A o posterior;
- GX Works3, a la versión 1.072A o posterior.

Para los productos que no tienen parche por el momento, se recomienda:

- Instalar la versión parcheada de GX Works3 en el ordenador que ejecuta alguno de los productos afectados para la comunicación con MELSEC.
- Ejecutar los productos afectados con una cuenta que no tenga privilegios de administrador.
- Instalar un *software* antivirus en el ordenador donde se ejecutan los productos afectados.
- Limitar al mínimo la exposición en la red de los equipos o sistemas de control y restringir el acceso a ellos desde redes o *hosts* no confiables.
- Utilizar *firewalls* para aislar el entorno TO del TI.
- Utilizar una VPN para cuando el acceso remoto sea necesario.

Detalle:

Aprovechando una vulnerabilidad de desbordamiento de búfer o una gestión inadecuada del parámetro de longitud, un atacante podría causar una condición de denegación de servicio al hacer un *spoofing* de los equipos MELSEC, FREQROL o GOT y enviar paquetes de respuesta especialmente diseñados. Se han asignado los identificadores CVE-2021-20587 y CVE-2021-20588 para cada una de las vulnerabilidades.

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

---

Múltiples vulnerabilidades en productos de Secomea

Fecha de publicación: 23/02/2021

Importancia: Alta

Recursos afectados:

- GateManager, todas las versiones anteriores a la 9.4;
- SiteManager, todas las versiones anteriores a la 9.4.

Descripción:

Tenable ha reportado dos vulnerabilidades de severidad alta y otra de severidad media que podrían permitir a un atacante inyectar código XSS, acceder a información confidencial o instalar puertas traseras en el dispositivo, respectivamente.

Solución:

Actualizar a la versión 9.4 siguiendo las referencias adicionales para GateManager y SiteManager.

Detalle:

- Una vulnerabilidad de XSS reflejado relacionada con el parámetro 'op' en *gui.cgi* de GateManager, podría permitir a un atacante inyectar código JavaScript arbitrario para que se ejecute en el navegador del usuario al navegar a la URL especialmente diseñada. Se ha asignado el identificador CVE- 2020-29028 para esta vulnerabilidad de severidad media.
- Una vulnerabilidad podría permitir a un atacante obtener información confidencial de la URL de ruta de todas las peticiones POST/GET después de que un usuario se haya autenticado en GateManager, ya que el *token* de autenticación queda expuesto de forma predeterminada. Se ha asignado el identificador CVE-2020-29030 para esta vulnerabilidad de severidad alta.
- Una vulnerabilidad en SiteManager podría permitir a un atacante, con permisos de nivel de operador de servicio, instalar *firmware* manipulado y así, instalar una puerta trasera en el dispositivo.

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

---

Múltiples vulnerabilidades en productos Advantech

Fecha de publicación: 24/02/2021

Importancia: Crítica

Recursos afectados:

- *Switches* ethernet industriales BB-ESWGP506-2SFP-T, versiones 1.01.09 y anteriores;
- router industrial Spectre RT ERT351, versiones de *firmware* 5.1.3 y anteriores.

Descripción:

Advantech ha publicado múltiples vulnerabilidades en sus productos que podrían permitir a un atacante ejecutar código arbitrario, divulgar información y borrar archivos.

Solución:

- El producto BB-ESWGP506-2SFP-T se encuentra fuera de su vida útil, el fabricante recomienda sustituirlo por un modelo posterior, por ejemplo el EKI-7708-4FPI;
- para Spectre RT ERT351, actualizar a la versión 6.2.7 o posteriores.

Detalle:

- El uso de contraseñas embebidas podría permitir a un atacante ganar acceso no autorizado y ejecutar código arbitrario. Se ha asignado el identificador CVE-2021-22667 para esta vulnerabilidad.
- La falta de neutralización de los caracteres especiales en la respuesta de error, podría permitir a los atacantes llevar a cabo ataques del tipo XSS reflejado. Se ha asignado el identificador CVE-2019-18233 para esta vulnerabilidad.
- El inicio de sesión y la contraseña se transmiten en texto claro, lo que podría permitir a un atacante interceptar la solicitud. Se ha asignado el identificador CVE-2019-18231 para esta vulnerabilidad.
- Los parámetros insuficientes de autenticación requeridos en el inicio de sesión para la aplicación web, podrían permitir a un atacante obtener un acceso completo utilizando un ataque de fuerza bruta a la contraseña. Se ha asignado el identificador CVE-2019-18235 para esta vulnerabilidad.
- La utilización de una versión obsoleta del cifrado de contraseñas de BusyBox, podría permitir a un atacante descubrir las contraseñas. Se han asignado los identificadores CVE-2018-20679, CVE-2016-6301 y CVE-2015-9261 para esta vulnerabilidad.
- La utilización de una versión no actualizada de OpenSSL, podría permitir a un atacante explotar vulnerabilidades conocidas en OpenSSL. Se han asignado los identificadores CVE-2016-2842, CVE-2016-0799 y CVE-2016-6304 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, SSL/TLS, Vulnerabilidad

---

Hash de contraseñas débil en la plataforma de servicios FactoryTalk de Rockwell Automation

Fecha de publicación: 24/02/2021

Importancia: Crítica

Recursos afectados:

Plataforma de servicios FactoryTalk, versiones 6.10.00 y 6.11.00.

Descripción:

Rockwell Automation ha reportado al CISA una vulnerabilidad de severidad crítica que podría permitir a un atacante remoto modificar o eliminar la configuración o datos de una aplicación.

Solución:

Actualizar el *software* a la nueva versión descargándola del sitio web de Rockwell Automation.

Detalle:

Un esfuerzo computacional insuficiente en la implementación del algoritmo de hash SHA-256 con la plataforma de servicios FactoryTalk impide que la contraseña de un usuario se cifre correctamente, con lo que un atacante remoto y no autenticado podría crear nuevos usuarios en la consola de gestión de la plataforma y así, modificar o eliminar la configuración o datos de una aplicación conectada a la misma. Se ha asignado el identificador CVE- 2020-14516 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, IoT, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Bosch

Fecha de publicación: 25/02/2021

Importancia: Alta

Recursos afectados:

- Rexroth IoT Gateway en las variantes IndraControl PR21: PR2100.1-*-IOTNN;
- ctrlX CORE Runtime, versión anterior a XCR-V-0108.

Descripción:

Las vulnerabilidades en las versiones del *kernel* de Linux y *sudo*, utilizadas en ctrlX CORE y en IoT Gateway, podrían permitir a un atacante con acceso a través de un terminal o Secure shell (SSH), la escalada de privilegios o realizar ataques de uso de la memoria previamente liberada.

Solución:

- Actualizar a la próxima versión, ctrlX CORE V0108, en cuanto sea posible. El fabricante recomienda encarecidamente dejar SSH desactivado y habilitarlo sólo temporalmente cuando sea necesario. Sólo los usuarios seleccionados deberían tener acceso a SSH a través del grupo "sshuser".
- En el IoT Gateway, la única cuenta de usuario del sistema ya tiene privilegios de superusuario y, por defecto, no existen otras cuentas. Se recomienda cambiar la contraseña por defecto y mantenerla en secreto. Se requieren medidas compensatorias para mitigar el riesgo. Se recomienda encarecidamente aplicar las medidas descritas en la 'Guía de seguridad de accionamientos y controles eléctricos'.

Detalle:

- Un problema de bloqueo en el subsistema *tty* del kernel de Linux, versiones 5.9.13 y anteriores, podría permitir un ataque de uso de la memoria previamente liberada *(use-after-free)* contra TIOCSPGRP, también conocido como CID-54ffccbf053b. Se ha asignado el identificador CVE-2020-29661 para esta vulnerabilidad.
- Una vulnerabilidad de desbordamiento de búfer basado en Heap, presente en sudo, podría permitir la escalada de privilegios a root a través de "sudoedit -s" y un argumento de línea de comandos que termina con un solo carácter de barra invertida. Se ha asignado el identificador CVE-2021-3156 para esta vulnerabilidad ya publicada en INCIBE-CERT.

Etiquetas: Actualización, Infraestructuras críticas, IoT, Vulnerabilidad

---

Múltiples vulnerabilidades en FvDesigner de Fatek

Fecha de publicación: 26/02/2021

Importancia: Alta

Recursos afectados:

FvDesigner, versión 1.5.76 y anteriores.

Descripción:

Francis Provencher {PRL} y *rgod*, en colaboración con ZDI de Trend Micro, han reportado 5 vulnerabilidades, todas de severidad alta, que podrían permitir a un atacante leer/modificar información, ejecutar código arbitrario o bloquear la aplicación.

Solución:

Fatek es consciente del problema y está desarrollando una solución. Para más información, contactar con Fatek por correo electrónico o por teléfono: 886-2-2808-2192.

Hasta entonces, CISA recomienda aplicar las siguientes medidas de protección básicas:

- Abrir sólo los archivos de proyecto de fuentes de confianza.
- Seguir el principio del usuario con menos privilegios.
- No hacer clic en enlaces web ni abrir archivos adjuntos no solicitados en mensajes de correo electrónico.
- Consultar cómo evitar las estafas por correo electrónico.
- Consultar más información de ataques de ingeniería social.

Detalle:

Un atacante podría crear un archivo de proyecto, especialmente diseñado, que le permitiría realizar una ejecución de código arbitrario si aprovechase alguna de las siguientes vulnerabilidades:

- Se ha identificado un problema de uso de memoria después ser liberada (*use after free*) en el procesamiento de los archivos de proyecto. Se ha asignado el identificador CVE-2021-22662 para esta vulnerabilidad.
- Un puntero no inicializado podría ser explotado mientras la aplicación procesa archivos de proyecto. Se ha asignado el identificador CVE-2021-22670 para esta vulnerabilidad.
- El producto afectado es vulnerable a un desbordamiento del búfer basado en la pila (*stack*) mientras se procesan los archivos de proyecto. Se ha asignado el identificador CVE-2021-22666 para esta vulnerabilidad.
- El producto afectado es vulnerable a una escritura fuera de límites al procesar archivos de proyecto. Se ha asignado el identificador CVE-2021-22683 para esta vulnerabilidad.
- El producto afectado es vulnerable a una lectura fuera de límites al procesar archivos de proyecto. Se ha asignado el identificador CVE-2021-22638 para esta vulnerabilidad.

Etiquetas: Infraestructuras críticas, Vulnerabilidad

Evasión de autenticación en múltiples productos de Rockwell Automation

Fecha de publicación: 26/02/2021

Importancia: Crítica

Recursos afectados:

Están afectados los siguientes productos de *software*:

- RSLogix 5000: versiones desde la 16 hasta la 20;
- Studio 5000 Logix Designer: versiones 21 y posteriores.

Los siguientes productos Rockwell Logix Controllers:

- CompactLogix 1768,
- CompactLogix 1769,
- CompactLogix 5370,
- CompactLogix 5380,
- CompactLogix 5480,
- ControlLogix 5550,

- ControlLogix 5560,
- ControlLogix 5570,
- ControlLogix 5580,
- DriveLogix 5560,
- DriveLogix 5730,
- DriveLogix 1794-L34,
- Compact GuardLogix 5370,
- Compact GuardLogix 5380,
- GuardLogix 5570,
- GuardLogix 5580,
- SoftLogix 5800.

Descripción:

Investigadores del laboratorio Information Systems Security Assurance, de la universidad de Soonchunhyang, y las empresas Kaspersky y Claroty, han descubierto una vulnerabilidad en la autenticación de los controladores Logix que permitiría evadir la autenticación de manera remota y alterar la configuración del controlador o el código de la aplicación.

Solución:

Rockwell aconseja a sus clientes combinar sus recomendaciones específicas, con las pautas generales de seguridad para una estrategia integral de defensa en profundidad, en particular:

- guía de instalación o implementación para CIP Security;
- consultar las pautas de diseño de seguridad de sistemas de Rockwell Automation sobre cómo utilizar sus productos;
- controles de seguridad y segmentación de red adecuados, consultando la Guía de implementación y diseño de Ethernet en toda la planta convergente (CPwE) para conocer las mejores prácticas para implementar la segmentación de la red.

Rockwell recomienda a los usuarios las siguientes acciones específicas para sus productos y versiones:

- ControlLogix 5580 v32 o posterior:
  - Ponga el interruptor de modo del controlador en modo "Ejecutar". Si no es posible, se recomiendan las siguientes mitigaciones:
    - Implemente CIP Security para las conexiones de Logix Designer a través del puerto frontal. CIP Security evita la conexión no autorizada cuando se implementa correctamente.
    - Si no usa el puerto frontal, use un módulo 1756-EN4TR ControlLogix Ethernet / IP e implemente CIP Security. El 1756-EN4TR es compatible con CIP Security, que evita conexiones no autorizadas cuando se implementa correctamente.
- ControlLogix 5580 v31:
  - Ponga el interruptor de modo del controlador en modo "Ejecutar". Si no es posible, se recomiendan las siguientes mitigaciones:
    - Aplique v32 o posterior y siga las acciones de mitigación descritas anteriormente.
    - Si no puede aplicar una versión más reciente, use un módulo 1756-EN4TR ControlLogix EtherNet / IP e implemente CIP Security. El 1756-EN4TR es compatible con CIP Security, que evita conexiones no autorizadas cuando se implementa correctamente.
- ControlLogix 5570 v31 o posterior:
  - Ponga el interruptor de modo del controlador en modo "Ejecutar". Si no es posible, se recomiendan las siguientes mitigaciones:
    - Utilice un módulo 1756-EN4TR ControlLogix EtherNet / IP e implemente CIP Security. El 1756-EN4TR es compatible con CIP Security, que evita conexiones no autorizadas cuando se implementa correctamente.
- ControlLogix 5580 v28-v30, ControlLogix 5570 v18 o posterior, ControlLogix 5560 v16 o posterior, ControlLogix 5550 v16, GuardLogix 5580 v31 o posterior, GuardLogix 5570 v20 o posterior, GuardLogix 5560 v16 o posterior, 1768 CompactLogix v16 o posterior, 1769 CompactLogix v16 o posterior, CompactLogix 5370 v20 o posterior, CompactLogix 5380 v28 o posterior, CompactLogix 5480 v32 o posterior, Compact GuardLogix 5370 v28 o posterior, Compact GuardLogix 5380 v31 o posterior, FlexLogix 1794-L34 v16, DriveLogix 5370 v16 o posterior:
  - Ponga el interruptor de modo del controlador en modo "Ejecutar".
- SoftLogix 5800: No hay mitigación adicional disponible. Siga la Guía de diseño e implementación de Converged Plantwide Ethernet (CPwE).

Adicionalmente, Rockwell recomienda que los usuarios empleen los siguientes métodos para detectar cambios en la configuración de los dispositivos:

- Supervise el registro de cambios del controlador para detectar modificaciones inesperadas o actividad anómala.
- Si usa v17 o posterior, utilice la función de registro del controlador.
- Si usa v20 o posterior, utilice la detección de cambios en la aplicación Logix Designer.
- Si está disponible, use la funcionalidad en Factory Talk AssetCentre para detectar cambios.

Para solicitudes de información adicional se pueden enviar a Rockwell RASecure Inbox: .

CISA también recomienda:

- Minimice la exposición de la red para todos los dispositivos, en especial desde Internet.
- Ubique las redes del sistema de control y los dispositivos remotos detrás de firewalls, y separados de la red empresarial.
- Cuando se requiera acceso remoto, utilice métodos seguros, como redes privadas virtuales (VPN).

Detalle:

La vulnerabilidad descubierta permite, a través de una funcionalidad en Studio 5000 Logix Designer, usar una clave para verificar que los controladores Logix se estén comunicando con los productos de Rockwell afectados, y un atacante remoto no autenticado podría eludir este mecanismo de verificación y autenticarse con los controladores. La criticidad de esta vulnerabilidad es de 10 según la metodología de cálculo CVSS v3. Se ha asignado el identificador CVE-2021-22681 para esta vulnerabilidad.

Etiquetas: 0day, Comunicaciones, Infraestructuras críticas, SCADA, Vulnerabilidad

Múltiples vulnerabilidades en OpenVPN-Client de PerFact

Fecha de publicación: 26/02/2021

Importancia: Alta

Recursos afectados:

OpenVPN-Client, versiones 1.4.1.0 y anteriores.

Descripción:

Sharon Brizinov, de Claroty, ha reportado al CISA estas vulnerabilidades, de severidad alta, que podría permitir a un atacante la escalada de privilegios local o la ejecución remota de código.

Solución:

Actualizar a la versión 1.6.0.

Detalle:

Un atacante podría aprovecharse de la arquitectura y enviar el comando *config* desde cualquier aplicación que se ejecute en el equipo anfitrión local para forzar al servidor *backend* a inicializar una nueva instancia de open-VPN con una configuración de open-VPN arbitraria. Esto podría resultar en la ejecución de comandos con privilegios del usuario SYSTEM. Se ha asignado el identificador CVE-2021-27406 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Control de acceso inapropiado en gateways de ProSoft Technology

Fecha de publicación: 26/02/2021

Importancia: Alta

Recursos afectados:

- ICX35-HWC-A, versiones 1.9.62 y anteriores;
- ICX35-HWC-E, versiones 1.9.62 y anteriores.

Descripción:

El investigador Maxim Rupp ha reportado al CISA una vulnerabilidad de severidad alta que podría permitir a un atacante remoto modificar la contraseña de usuario, cambiar la configuración del equipo o detener el funcionamiento del mismo.

Solución:

Actualizar el *firmware* a la versión 1.10.30 u otra posterior.

Detalle:

Un atacante remoto o un proceso externo podría cambiar la contraseña actual a través de la interfaz web de las pasarelas (*gateways*), dado que no se solicita la contraseña actual para ello. Se ha asignado el identificado CVE-2021-22661 para esta vulnerabilidad.

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