Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Marzo - 2024

Sobre Axus

Axus es una empresa especializada en ciberseguridad, con presencia en el Perú y Latinoamérica. Asesora a clientes en la protección de su información e infraestructura tanto en ámbitos industriales (OT) como en ámbitos corporativos (IT) y viene registrando una creciente participación en el ámbito de Internet de las Cosas (IoT) y en la protección de entornos Cloud e Híbridos.

En base a su reputación como especialista con los principales fabricantes de la industria y su equipo profesional en permanente capacitación, Axus genera valor a través de una visión consultiva que busca definir soluciones a la medida de las necesidades de cada cliente.

Alertas de Ciberseguridad

A continuación, compartimos con ustedes algunas de las alertas más relevantes de marzo.

Alertas de Seguridad IT:

- Nueva Modalidad de Ataque a Correo Electrónico Mediante Explotación de DNS
- El Ministerio de Defensa y el Ejército del Perú Bajo Ciberataques
- Más de 100 Organizaciones de EE. UU. y Europa Fueron el Objetivo de Ataques de Malware de StrelaStealer
- Más de 100,000 Personas Afectadas por Ataque de Ransomware a Nissan

Alertas de Seguridad OT/ICS:

- Claroty's Team82 Descubre Vulnerabilidades Cruciales en Dispositivos UniStream de Unitronics, Impulsando Actualizaciones del Proveedor
- Diez vulnerabilidades encontradas en productos de Rockwell Automation

Nueva Modalidad de Ataque a Correo Electrónico Mediante Explotación de DNS

Tipo de Ataque: **Phishing**

Medio de Propagación: **Correo electrónico**

1. **RESUMEN:**

La adopción de DMARC es esencial para garantizar la autenticación del correo electrónico y prevenir ataques maliciosos. Sin embargo, una nueva campaña llamada SubdoMailing está explotando la complacencia en su implementación, enviando correos maliciosos desde dominios comprometidos. Los atacantes aprovechan registros obsoletos para evadir controles SPF.

2. **DETALLE:**

Durante años, expertos en seguridad han alentado a adoptar DMARC para fortalecer la autenticación del correo electrónico. La campaña SubdoMailing ha surgido como un nuevo tipo de ataque que explota la complacencia de las organizaciones en la implementación superficial de DMARC. Esta campaña envía correos maliciosos desde dominios y subdominios comprometidos debido a adquisiciones de dominios y problemas de DNS no resueltos.

Guardio Labs informó sobre 8,000 dominios y 13,000 subdominios utilizados en estos ataques desde 2022. Red Sift, socio de DMARC de Cisco, también detectó incidentes similares, lo que llevó a descubrir la explotación de registros DNS obsoletos o mal configurados.

Los atacantes aprovechan estos registros para enviar correos fraudulentos que a menudo pasan los controles SPF, utilizando subdominios no relacionados con el dominio principal. Es crucial que las organizaciones supervisen activamente estos problemas.

Se recomienda evitar que los nombres de dominio caduquen, mantener un DNS limpio eliminando registros no utilizados y verificar la autenticidad de los remitentes de correo electrónico. Además, se aconseja monitorear de cerca los envíos de correo electrónico desde los dominios propios para detectar cualquier actividad sospechosa lo antes posible.

3. **RECOMENDACIONES:**
   - Monitorear subdominios que puedan estar relacionados con su organización.
   - Emplear un servicio de monitoreo de marca que revisa de forma permanente y proactiva dominios similares al de la organización.

4. **REFERENCIAS:**
   - https://blogs.cisco.com/security/hiding-in-plain-sight-how-subdomain-attacks-use-your-email-authentication-against-you?utm_medium=feed&utm_source=feedpress.me&utm_campaign=Feed%3A+CiscoSecurity

El Ministerio de Defensa y el Ejercito del Perú Bajo Ciberataques

Tipo de Ataque: Ransomware.

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Servidores de archivos
   - Página Web
   - Probablemente otros, que no han sido revelados.

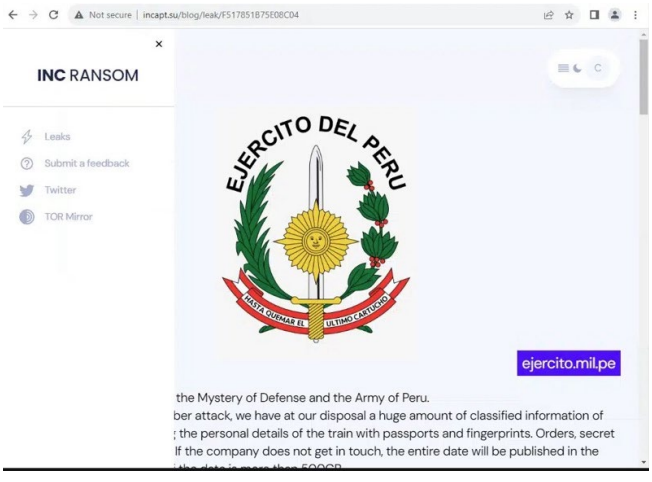
2. **RESUMEN:**

Recientemente, dos grupos de ciberatacantes han proclamado el éxito de sus ataques contra instituciones gubernamentales en Perú. INC Ransom afirmó haber logrado infiltrarse en el Ministerio de Defensa y el Ejército del país, obteniendo acceso a más de 500 GB de información. Por otra parte, el grupo RansomExx publicó en su página web que han obtenido más de 700 GB de datos sustraídos del Ministerio de Defensa peruano.

3. **DETALLE:**

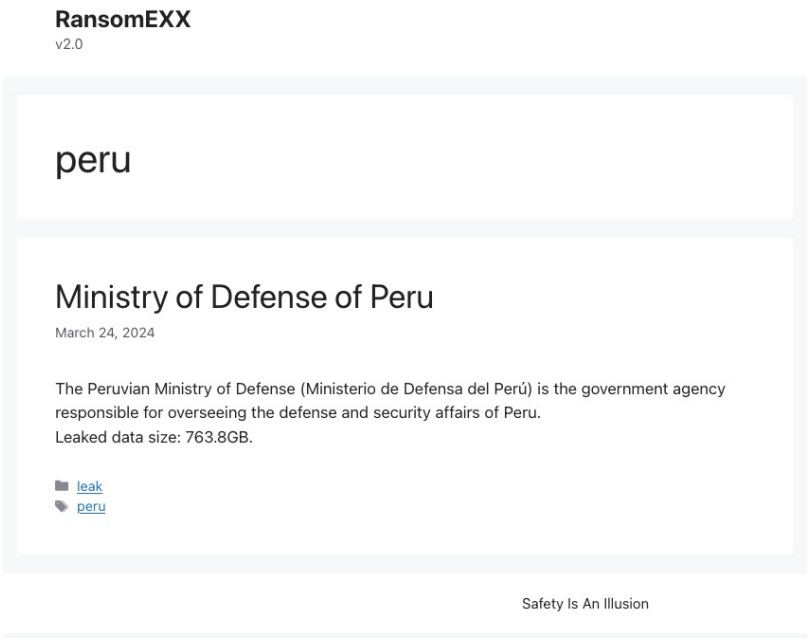
Durante la semana del 25 de marzo, dos grupos de cibercriminales han anunciado el éxito de sus ataques contra el Ministerio y el Ejército del Perú, logrando acceder a información confidencial.

El grupo de ciberdelincuentes conocido como INC Ransom perpetró un ciberataque contra el Ministerio de Defensa y el Ejército del Perú, obteniendo información confidencial que incluye pasaportes, datos personales de los miembros, huellas dactilares, órdenes y documentos clasificados, entre otros. Según su página web, la cantidad de datos supera los 500 GB, y han publicado imágenes de documentos oficiales y datos personales como prueba. El grupo está exigiendo que las autoridades se pongan en contacto con ellos lo antes posible; de lo contrario, amenazan con publicar toda la información. Hasta el momento, no se tiene conocimiento de si ha habido conversaciones entre las partes involucradas.



Página Web de INC Ransom

Por su parte, RansomExx ha actualizado su página web para incluir al Ministerio del Perú en su lista de víctimas. En la información publicada, detallan que han obtenido 763.8 GB de datos robados. Sin embargo, el monto exigido para evitar la publicación de esta información permanece desconocido.



Página Web de RansomExx

4. RECOMENDACIONES:

- Verificar o fortalecer las defensas antimalware, especialmente si se tiene comunicación con la entidad afectada.
- Verificar o fortalecer los mecanismos de recuperación como backups, especialmente si se tiene comunicación con la entidad afectada.
- Fortalecer la concientización de los empleados, especialmente si se mantienen comunicación con la entidad afectada.

5. REFERENCIAS:

- https://www.ransomfeed.it/
- https://www.ransomfeed.it/index.php?page=post_details&id_post=13949
- https://www.ransomfeed.it/index.php?page=post_details&id_post=13918

Más de 100 Organizaciones de EEUU y Europa Fueron el Objetivo de Ataques del Malware StrelaStealer

Tipo de Ataque: Malware.

Medio de Propagación: Internet

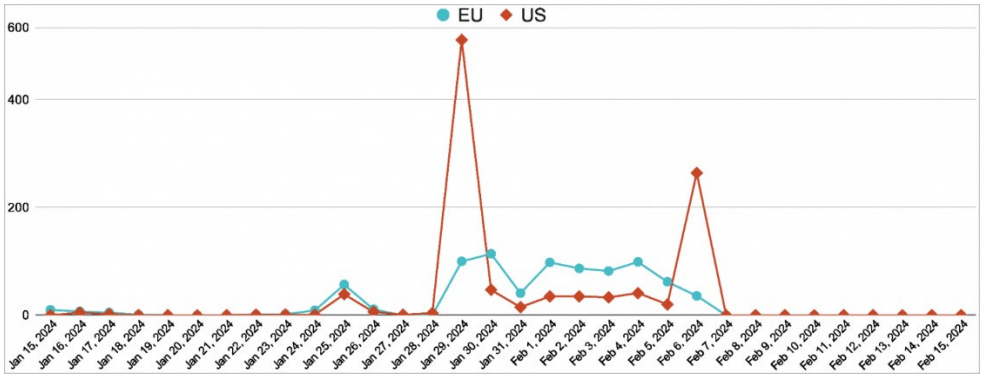
1. RESUMEN:

Durante los primeros meses del año se ha identificado una campaña masiva de StrelaStealer malware con el objetivo de robar credenciales de correos electrónicos, afectando a más de 100 organizaciones en EE.UU. y Europa.

2. DETALLE:

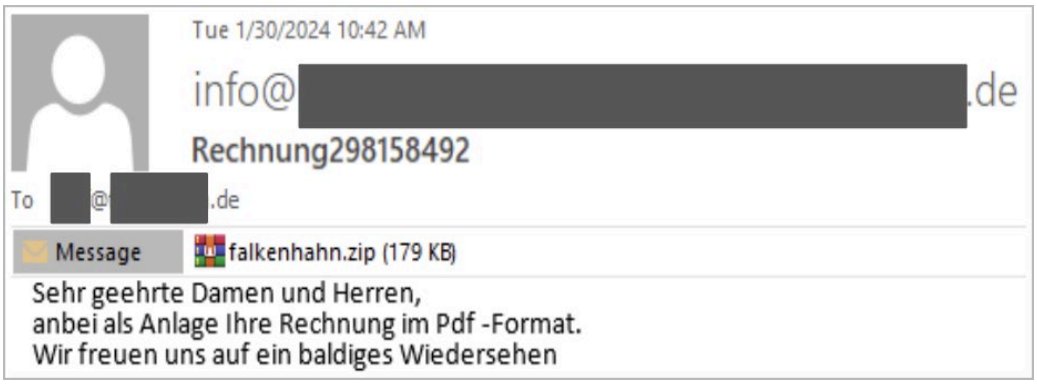
StrelaStealer es un malware que roba credenciales enfocado en correos electrónicos, se detectó por primera vez en septiembre del 2022. Este malware se caracteriza por usar método de infección de archivos en varios idiomas para evadir la protección y detección. Cuando se detectó por primera vez se en 2022, la campaña estaba dirigida principalmente a usuario hispanohablantes. Sin embargo, recientemente ha cambiado ya que el malware ahora se dirige a EE.UU. y Europa.

Según el informe de Unit42 de Palo Alto Networks, entre finales de enero y principios de febrero existió un elevado volumen de distribución de correos electrónicos de phishing. Durante estos días los ataques superaron los 500.



StrelaStealer últimos volúmenes de distribución (Unit42)

Las atacantes del malware personalizaban los correos de phishing en diferentes idiomas para evitar ser detectados.

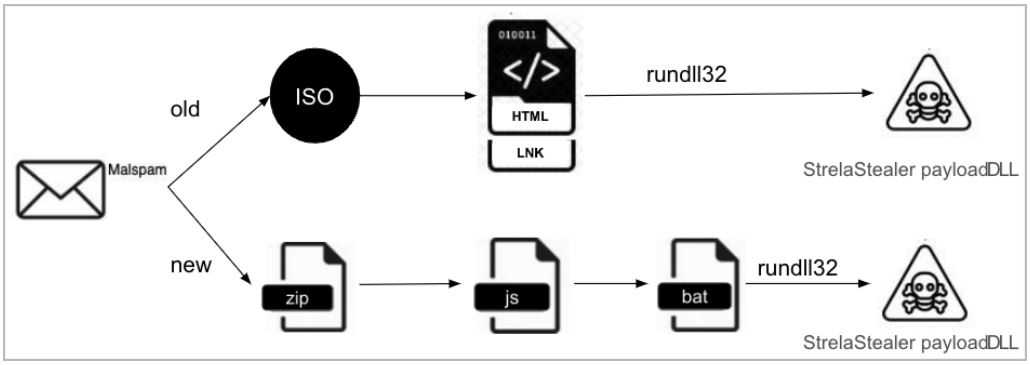


Correo electrónico con temática de factura escrito en alemán (Unidad42)

La evolución de los métodos de infección de StrelaStealer desde finales de 2022 ha sido notable, aunque el enfoque en correos electrónicos maliciosos como principal vía de infección continúa siendo predominante.

En versiones anteriores, los correos electrónicos solían adjuntar archivos .ISO que contenían un acceso directo .lnk y un archivo HTML. Estos archivos empleaban poliglotismo para invocar 'rundll32.exe' y ejecutar la carga útil del malware.

En su más reciente cadena de infección, se ha observado el uso de archivos ZIP adjuntos para distribuir archivos JScript en el sistema de la víctima. Al ejecutarse, estos scripts liberan un archivo por lotes y un archivo codificado en base64, que se descodifica en una DLL. Esta DLL es ejecutada nuevamente a través de 'rundll32.exe', implementando así la carga útil de StrelaStealer.



Viejas y nuevas cadenas de infección (Unidad 42)

3. **RECOMENDACIONES:**
   - Utilizar un antimalware robusto para analizar todas las descargas y archivos sospechosos. Este se debe mantener siempre actualizado y activo.
   - Mantener el sistema operativo, navegador y aplicaciones siempre actualizados a su última versión para evitar vulnerabilidades.
   - Utilizar contraseñas robustas y diferentes para proteger todas las cuentas. De preferencia, utilizar la autenticación multifactorial.
4. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/over-100-us-and-eu-orgs-targeted-in-strelastealer-malware-attacks/

Más De 100,000 Personas Afectadas por Ataque de Ransomware a Nissan

Tipo de Ataque: Ransomware.

Medio de Propagación: Internet

1. RESUMEN:

Nissan Motor Corporation y Nissan Financial Services en Australia y Nueva Zelanda sufrieron una intrusión cibernética el 5 de diciembre de 2023. El grupo de ransomware Akira se atribuyó el ataque y afirmó haber robado 100 GB de información, incluyendo archivos corporativos y datos personales. Nissan está notificando a aproximadamente 100,000 personas afectadas, que incluyen clientes, concesionarios y empleados actuales y anteriores de Nissan, así como clientes de otras marcas financieras asociadas

2. DETALLE:

El fabricante de automóviles informó que descubrió una intrusión el 5 de diciembre de 2023 y notificó a los clientes sobre un incidente cibernético disruptivo ese mismo día. El ataque afectó a Nissan Motor Corporation y Nissan Financial Services en Australia y Nueva Zelanda.

Posteriormente, el grupo de ransomware Akira se atribuyó la responsabilidad del ataque, declarando haber sustraído 100 GB de información de la empresa, que incluía archivos corporativos e información personal.

Desde entonces, los hackers han publicado archivos supuestamente sustraídos de los sistemas de Nissan, insinuando que el fabricante de automóviles se negó a satisfacer las demandas de rescate. En una actualización emitida el miércoles, Nissan Oceanía anunció que había comenzado a comunicarse con las personas afectadas.

Después de una investigación llevada a cabo con la colaboración de autoridades gubernamentales y expertos externos en ciberseguridad, la empresa ha determinado que la brecha de seguridad afecta a algunos clientes, concesionarios y empleados actuales y anteriores de Nissan.

Además, los clientes de las empresas financieras de las marcas Mitsubishi, Renault, Skyline, Infiniti, LDV y RAM también se ven afectados.

Nissan estima que necesita notificar a unas 100,000 personas, aunque el número real podría ser menor una vez que se validen los datos de contacto y se eliminen las entradas duplicadas de la lista.

"Nissan declaró: 'El tipo de información involucrada variará según la persona. Las estimaciones actuales sugieren que hasta el 10% de las personas han visto comprometida alguna forma de identificación gubernamental. El conjunto de datos incluye aproximadamente 4,000 tarjetas de Medicare, 7,500 licencias de conducir, 220 pasaportes y 1,300 números de declaración de impuestos. El 90% restante de las personas notificadas se ha visto afectado por algún otro tipo de información personal; esto incluye copias de extractos de transacciones relacionadas con préstamos para cuentas de préstamos, información de empleo o salario, o información general como fechas de nacimiento'".

A las personas afectadas se les ofrecen servicios gratuitos de monitoreo de crédito y protección contra robo de identidad, y Nissan está reembolsando a quienes necesiten reemplazar su identificación gubernamental debido al incidente.

3. RECOMENDACIONES

- Verificar o fortalecer las defensas antimalware, especialmente si se tiene comunicación con la entidad afectada.
- Verificar o fortalecer los mecanismos de recuperación como backups, especialmente si se tiene comunicación con la entidad afectada.
- Fortalecer la concientización de los empleados, especialmente si se mantienen comunicación con la entidad afectada.

4. REFERENCIAS:

- https://www.securityweek.com/nissan-data-breach-affects-100000-individuals/

Claroty's Team82 Descubre Vulnerabilidades Cruciales en Dispositivos UniStream de Unitronics, Impulsando Actualizaciones del Proveedor

Tipo de Ataque: Vulnerabilidades

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - PLC y HMI Unitronics V570
2. **RESUMEN:**

Se descubrieron ocho vulnerabilidades en dispositivos UniStream de Unitronics que permiten a atacantes remotos eludir la autenticación y tomar el control completo del PLC, ejecutando comandos arbitrarios. Estos ataques se produjeron después de que dispositivos de Unitronics fueran objeto de ciberataques revelados en noviembre, lo que afectó a múltiples controladores Vision, incluyendo instalaciones de agua en los Estados Unidos. Un grupo conocido como CyberAv3ngers se atribuyó la responsabilidad de estos ataques.

3. **DETALLE:**

Los dispositivos integrados de controladores lógicos programables (PLCs) y las interfaces hombre-máquina (HMI) de Unitronics, un proveedor israelí, fueron el objetivo de preocupantes ataques cibernéticos desvelados en noviembre, los cuales impactaron en numerosos controladores Vision de Unitronics en diversas partes del mundo, incluyendo instalaciones de agua en los Estados Unidos que experimentaron alteraciones en su funcionamiento.

Un grupo autodenominado CyberAv3ngers se atribuyó la responsabilidad de estos ataques y advirtió que toda la tecnología desarrollada en Israel estaba bajo su radar. Un PLC/HMI comprometido de Unitronics, específicamente el modelo V570, en la Autoridad Municipal de Agua de Alquippa, fue objeto de vandalismo, indicando así que los atacantes, al menos, lograron acceder al dispositivo.

Este incidente impulsó a la Agencia de Ciberseguridad e Infraestructura (CISA) a emitir una alerta en la que recomendaba a los usuarios cambiar las contraseñas predeterminadas en los productos de Unitronics, cerrar los puertos que exponen directamente estos dispositivos a Internet y asegurar cualquier acceso remoto a través de una VPN o una solución de acceso remoto segura. Unitronics también parcheó la vulnerabilidad utilizada en este ataque en la versión 9.9.00 del producto Vision afectado.

Como resultado de este suceso, el equipo de investigación Team82 decidió examinar la superficie de ataque de la serie de PLC UniStream, la última generación de PLCs y HMIs integrados de Unitronics. Entre las mejoras implementadas en esta serie UniStream se encuentra un esquema de autenticación nativo que el equipo de Team82 logró evadir.

Durante el proceso de investigación, se identificaron ocho vulnerabilidades que no solo burlaron las funciones de autenticación y autorización en los PLC UniStream, sino que además pudieron ser concatenadas para lograr la ejecución remota de código en el dispositivo. Utilizando servicios de escaneo de Internet disponibles públicamente, se localizaron alrededor de 480 dispositivos UniStream expuestos a Internet y vulnerables.

Team82 comunicó de manera confidencial estas vulnerabilidades a Unitronics, CISA y la Dirección Nacional de Ciberseguridad de Israel, la cual emitió una advertencia instando a los usuarios a actualizar sus dispositivos y limitar su exposición directa a Internet.

4. RECOMENDACIONES:

- Actualizar sus dispositivos UniStream a la última versión estable recomendada.

5. REFERENCIAS:

- https://industrialcyber.co/news/clarotys-team82-reveals-critical-vulnerabilities-in-unitronics-unistream-devices-prompting-vendor-updates/
- https://claroty.com/team82/blog/new-critical-vulnerabilities-in-unitronics-unistream-devices-uncovered

Diez Vulnerabilidades Encontradas en Productos de Rockwell Automation

Tipo de Ataque: Vulnerabilidades

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- Rockwell Automation Factory Talk View ME
- Rockwell Automation Arena Simulation
- Rockwell Automation PowerFlex 527

2. RESUMEN:

Recientemente, la agencia de ciberseguridad e infraestructura de los E.E.U.U., también conocida como CISA por sus siglas en inglés, publico 4 avisos acerca de vulnerabilidades detectadas en sistemas de controles industriales (ICS) del fabricante Rockwell Automation.

3. DETALLE:

Dentro del primer aviso publicados por la CISA, se encuentran cinco vulnerabilidades de ejecución de código arbitrario de alta gravedad y un problema de divulgación de información y denegación de servicio (DoS) de gravedad media, encontrados en el producto Rockwell Automation Arena Simulation. Para la explotación de estas vulnerabilidades es necesario que el usuario descargue y abra un archivo malicioso.

Vulnerabilidades de Rockwell Automation Arena Simulation:

Categoría	Impacto	CVSS base score	CVSS vector	CVE Numbers
Out-of-bounds Write CWE-787	Inserción de código malicioso, para provocar una infracción de acceso. Afectando la confidencialidad, integridad y disponibilidad del producto	8.4	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	CVE-2024-21912
HEAP-BASED BUFFER OVERFLOW CWE-122		8.4	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	CVE-2024-21913
Improper Restriction of Operations within the Bounds of a Memory Buffer CWE-119		8.4	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	CVE-2024-2929
Use After Free CWE-416		8.4	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	CVE-2024-21918
Out-of-bounds Read CWE-125		8.4	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	CVE-2024-21919

Out-of-bounds Read CWE-125	Podría revelar información confidencial e incluso provocar que la aplicación falle	4.6	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N	CVE-2024-21920

En el segundo aviso de la CISA, es sobre tres vulnerabilidades detectadas en el producto PowerFlex, que al ser explotadas pueden ser usadas para generar un ataque de denegación de servicios, DoS. Hasta la publicación de este boletín aún no existe un parche para esta vulnerabilidad.

Vulnerabilidades de Rockwell PowerFlex 527:

Categoría	Impacto	CVSS base score	CVSS vector	CVE Numbers
Improper Input Validation CWE-120	El servidor web puede fallar y necesitar un reinicio manual	8.7	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N	CVE-2024-2425
Improper Input Validation CWE-120	Puede generar una disrupción en la comunicación CIP y necesitar un reinicio manual	8.7	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N	CVE-2024-2426
Uncontrolled Resource Consumption CWE-400	Si se envían varios paquetes de datos al dispositivo repetidamente, el dispositivo fallará y requerirá un reinicio manual	8.7	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N	CVE-2024-2427

El tercer aviso es acerca de una vulnerabilidad de seguridad de gravedad média descubierto por RockWell.

Vulnerabilidades de Rockwell PowerFlex 527:

Categoría	Impacto	CVSS base score	CVSS vector	CVE Numbers
Neutralización inadecuada de la entrada durante la generación de la página web ("Cross-site Scripting") CWE-79	Puede provocar la pérdida de visión o control de producto PanelView	6.9	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N	CVE-2024-21914

4. RECOMENDACIONES:

- Se recomienda actualizar los productos Arena y FactoryTalk View ME afectados a la versión de software recomendada por el fabricante.
- En el caso de PowerFlex 527, que hasta la fecha de publicación de este boletín, esta sin parche, por lo cual se recomienda realizar acciones de mitigación de riesgos.

5. REFERENCIAS:

- **https://www.cisa.gov/news-events/alerts/2024/03/26/cisa-releases-four-industrial-control-systems-advisories**
- **https://www.cisa.gov/news-events/ics-advisories/icsa-24-086-02**
- **https://www.cisa.gov/news-events/ics-advisories/icsa-24-086-03**
- **https://www.cisa.gov/news-events/ics-advisories/icsa-24-086-04**

Titulo

Tipo de Ataque: Vulnerabilidades

Medio de Propagación: Internet

6. PRODUCTOS AFECTADOS:

- Productos

7. RESUMEN:

En la segunda

8. DETALLE:

Siemens

9. RECOMENDACIONES:

- Aplicar

10. REFERENCIAS:

- https://www.securityweek.com/siemens-schneider-electric-release-first-ics-patch-tuesday-advisories-of-2024/