Alerta de Seguridad

Riesgo de vulnerabilidades IT y OT

Agosto-2023

Sobre Axus

Axus es una empresa líder 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 Agosto.

Alertas de Seguridad IT:

- Relojera japonesa Seiko vulnerada por banda de ransomware BlackCat.
- El grupo de ransomware Cuba explota Veeam para atacar infraestructuras críticas.
- Vulnerabilidad crítica de Citrix ShareFile explotada ampliamente.

Alertas de Seguridad OT/ICS:

- Los ataques de ransomware a organizaciones industriales se duplicaron el año pasado.
- PLC industriales en todo el mundo afectados por fallas en CODESYS V3 RCE.
- Vulnerabilidad alta en Armor PowerFlex de Rockwell Automation.

Relojera japonesa Seiko vulnerada por banda de ransomware BlackCat

Tipo de Ataque: Ransomware

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- Base de datos.

2. RESUMEN:

El grupo de ransomware BlackCat/ALPHV ha dirigido un ataque a la prestigiosa marca de relojes japonesa Seiko, y ha reclamado la responsabilidad por este ciberataque en su sitio de extorsión. Seiko es uno de los fabricantes de relojes más grandes e históricos del mundo, con aproximadamente 12,000 empleados y una facturación anual que supera los $1.6 mil millones.

3. DETALLE:

Se cree El 10 de agosto de 2023, la compañía publicó un aviso sobre una brecha de datos, informando que un tercero no autorizado obtuvo acceso al menos a una parte de su infraestructura de tecnología de la información y accedió o extrajo datos.

"Al parecer, el 28 de julio de 2023, alguna(s) parte(s) aún no identificada(s) obtuvo/obtuvieron acceso no autorizado a al menos uno de nuestros servidores", dice el comunicado de Seiko.

"Posteriormente, el 2 de agosto, contratamos a un equipo de expertos externos en ciberseguridad para investigar y evaluar la situación."

"Como resultado, ahora estamos razonablemente seguros de que hubo una violación y que parte de la información almacenada por nuestra Compañía y/o nuestras empresas del Grupo pudo haber sido comprometida."

Seiko se disculpó con los potencialmente afectados, ya sean clientes o socios comerciales, y les instó a estar alerta ante posibles intentos de correo electrónico u otras comunicaciones que pudieran hacerse pasar por Seiko.

El grupo de ransomware BlackCat afirmó ser el responsable del ataque a Seiko, publicando muestras de datos que afirman haber robado durante el ataque.

En la lista, los actores amenazantes se burlan de la seguridad informática de Seiko y filtran lo que parecen ser planes de producción, escaneos de pasaportes de empleados, planes de lanzamiento de nuevos modelos y resultados de pruebas de laboratorio especializadas.

Lo más preocupante es que los actores de amenaza han filtrado muestras de lo que afirman son esquemas técnicos confidenciales y diseños de relojes Seiko.

Esto indica que BlackCat muy probablemente posee dibujos que muestran componentes internos de Seiko, incluida tecnología patentada, lo cual sería perjudicial publicar y exponer a competidores e imitadores.

BlackCat es uno de los grupos de ransomware más avanzados y notorios que se dirige activamente a empresas, y constantemente evoluciona sus tácticas de extorsión.

Por ejemplo, el grupo fue el primero en usar un sitio web clearweb dedicado a filtrar datos de una víctima en particular y, más recientemente, creó una API de filtración de datos, lo que facilita la distribución de información robada.

El grupo viene siendo observado desde 2021, en que es pionero en usar el lenguaje Rust, que favorece evadir los controles de detección convencionales. También es uno de los primeros en posicionarse como RaaS (Ransomware as a Service).

El 21/8/23, investigadores de Curated Intel informaron que un intermediario de acceso inicial (IAB) estaba vendiendo acceso a una empresa manufacturera japonesa el 27 de julio, un día antes de que Seiko dijera que se vio comprometida inicialmente.

Aunque el IAB no compartió el nombre de la empresa a la que estaban vendiendo acceso, dijeron que la empresa se dedica a la manufactura y tiene unos ingresos de '1.8B' según Zoominfo, lo cual coincide exactamente con la página de Zoominfo de Seiko.

4. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/japanese-watchmaker-seiko-breached-by-blackcat-ransomware-gang/#google_vignette
- The many lives of BlackCat ransomware | Microsoft Security Blog
- El nuevo ransomware BlackCat | Blog oficial de Kaspersky
- Breaking Down the BlackCat Ransomware Operation (cisecurity.org)

Vulnerabilidad crítica de Citrix ShareFile explotada ampliamente

Tipo de Ataque: Ransomware

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**

- Citrix ShareFile

2. **RESUMEN:**

CISA (Agencia de Ciberseguridad e Infraestructura) advierte que una vulnerabilidad crítica en Citrix ShareFile para transferencia segura de archivos, rastreada como CVE-2023-24489, está siendo usada por actores desconocidos. La agencia ha añadido esta vulnerabilidad a su catálogo de fallas de seguridad conocidas que están siendo explotadas “in the wild”.

Citrix ShareFile (también conocido como Citrix Content Collaboration) es una solución SaaS de almacenamiento en la nube de transferencia de archivos gestionados, que permite a clientes y empleados cargar y descargar archivos de manera segura.

El servicio también ofrece una solución de 'Controlador de zonas de almacenamiento' que permite a las empresas configurar su almacenamiento de datos privado para alojar archivos, ya sea en el sitio o en plataformas en la nube compatibles, como Amazon S3 y Windows Azure.

3. **DETALLE:**

Esta El 13 de junio de 2023, ShareFile publicó un aviso de seguridad sobre una nueva vulnerabilidad en las zonas de almacenamiento de ShareFile rastreada como CVE-2023-24489, con una gravedad crítica de 9.8/10. Esta vulnerabilidad podría permitir que atacantes no autenticados comprometan zonas de almacenamiento gestionadas por el cliente.

"A través de nuestra investigación logramos lograr una carga de archivos arbitraria no autenticada y una ejecución remota de código completo explotando un error criptográfico aparentemente inocuo", explican los investigadores de AssetNote.

Utilizando esta falla, un actor de amenazas podría cargar un shell web en un dispositivo para obtener acceso completo al almacenamiento y a todos sus archivos.

Aunque CISA comparte esta misma advertencia en muchas alertas, las fallas que impactan a las soluciones de transferencia de archivos gestionados (MFT) son de particular preocupación, ya que los actores de amenazas las han explotado ampliamente para robar datos de empresas en ataques de extorsión.

Aunque aún no se ha relacionado públicamente la explotación de esta falla con el robo de datos, CISA ahora requiere que las agencias del Gobierno Federal apliquen parches para esta vulnerabilidad antes del 6 de septiembre de 2023.

4. **RECOMENDACIONES**
   - Es recomendable que todas las organizaciones apliquen los parches de seguridad apenas sean liberados.
5. **REFERENCIAS:**
   - CISA warns of critical Citrix ShareFile flaw exploited in the wild (bleepingcomputer.com)

El grupo de ransomware Cuba explota Veeam para atacar infraestructuras críticas

Tipo de Ataque: Ransomware

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**

- Veeam Backup & Replication

2. **RESUMEN:**

El grupo de ransomware Cuba ha atacado a una organización de infraestructura crítica en los Estados Unidos aprovechando una vulnerabilidad antigua en el software Veeam, según una investigación de BlackBerry. Este prolífico grupo de ransomware "desplegó un conjunto de herramientas maliciosas que se superponían con campañas anteriores asociadas a este atacante, además de introducir nuevas, incluido el primer uso observado de una vulnerabilidad de explotación para la vulnerabilidad CVE-2023-27532 de Veeam", informó BlackBerry.

3. **DETALLE:**

La vulnerabilidad, que afecta al software Veeam Backup & Replication, permite a un atacante potencialmente acceder a credenciales almacenadas en el archivo de configuración en dispositivos víctima.

El grupo de ransomware Cuba, que no tiene ninguna conexión conocida con la República de Cuba, había comprometido a más de 100 organizaciones en todo el mundo y había exigido más de $145 millones en rescate a fines de 2022, según un aviso conjunto emitido por el FBI y la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA). El agente de amenaza también atacó a un integrador de TI en América Latina en junio, lo que subraya el enfoque persistente del agente de amenaza en las organizaciones de infraestructura crítica a nivel mundial.

La campaña más reciente del grupo, motivada financieramente, se dirigió a organizaciones en Estados Unidos, México, Guatemala, Honduras, El Salvador, República Dominicana, Costa Rica, Panamá, Colombia, Ecuador y Chile, según BlackBerry. La investigación indica que el grupo de amenazas Cuba continúa apuntando a entidades en sectores cruciales como infraestructuras críticas. El grupo de ransomware fue descubierto por primera vez a fines de 2019 y había recibido $60 millones en pagos de rescate a fines de 2022, según la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA).

4. **RECOMENDACIONES:**
   - Se recomienda a las organizaciones contar con un equipo de Ciberinteligencia que este atento a las vulnerabilidades y en el parchado de estas.
5. **REFERENCIAS:**

   - Cuba ransomware group exploits Veeam to hit critical infrastructure | Cybersecurity Dive

Los ataques de ransomware a organizaciones industriales se duplicaron el año pasado

Tipo de Ataque: Ransomware

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- Sistemas de control industriales

2. RESUMEN:

El número de ataques de ransomware dirigidos a organizaciones industriales e infraestructuras se ha duplicado desde el segundo trimestre de 2022, según datos de la firma de ciberseguridad industrial Dragos.

En un informe que analiza datos del segundo trimestre de 2023, Dragos señaló que registró 253 incidentes de ransomware, un aumento del 18% respecto al primer trimestre de 2023, cuando observó 214 ataques.

3. DETALLE:

La compañía registró 189 incidentes de ransomware en el último trimestre de 2022, un aumento del 30% respecto a los 128 incidentes en el tercer trimestre de 2022. En el segundo trimestre de 2022, la cifra descendió a 125 desde los 158 incidentes en el primer trimestre. En ese momento, Dragos atribuyó la disminución al cierre de la operación Conti.

Dragos ha atribuido el aumento en los ataques al descenso en los ingresos por ransomware en 2022, ya que más víctimas se negaron a pagar.

"Dragos evalúa con moderada confianza que el tercer trimestre de 2023 presenciará un aumento de los ataques de ransomware que impactan en las organizaciones industriales por dos razones. En primer lugar, la tensión política prevaleciente entre los países de la OTAN y Rusia motiva a los grupos de ransomware alineados con Rusia a seguir apuntando y perturbando la infraestructura crítica en los países de la OTAN", dijo Dragos.

"En segundo lugar, a medida que disminuye el número de víctimas dispuestas a pagar rescates, los grupos RaaS (Ransomware as a Service) han cambiado su enfoque hacia organizaciones más grandes, recurriendo a ataques de distribución de ransomware generalizados para mantener sus ingresos", agregó.

Casi la mitad de los ataques de ransomware observados por la firma de seguridad afectaron a organizaciones e infraestructuras en América del Norte, seguido por Asia.

La mitad de los 66 grupos de ransomware monitoreados por Dragos lanzaron ataques en el segundo trimestre de 2023, siendo el más activo LockBit, responsable de 48 incidentes, seguido por Alpha V, con 31 incidentes, y Black Basta, con 26 incidentes.

El sector manufacturero sigue siendo el más afectado, con 177 incidentes, seguido por los sistemas de control industrial (ICS), el transporte y el petróleo y gas.

4. RECOMENDACIONES:

- Se recomienda contar con un equipo de ciberseguridad que pueda prevenir y/o contener este tipo de ataques y reducir los daños en las organizaciones.

5. REFERENCIAS:

- Ransomware Attacks on Industrial Organizations Doubled in Past Year: Report - SecurityWeek
- https://www.securityweek.com/ransomware-often-hits-industrial-systems-significant-impact-survey/
- https://www.securityweek.com/dragos-says-ransomware-hackers-failed-at-elaborate-extortion-scheme/
- https://www.securityweek.com/2022-ics-attacks-fewer-than-expected-on-us-energy-sector-but-ransomware-surged/

PLC industriales en todo el mundo afectados por fallas en CODESYS V3 RCE

Tipo de Ataque: Vulnerabilidad

Medio de Propagación: Red, Internet

1. **PRODUCTOS AFECTADOS:**
   - Controladores Lógicos Programables (PLC)
2. **RESUMEN:**

Millones de controladores lógicos programables (PLC) utilizados en entornos industriales en todo el mundo están en riesgo debido a 15 vulnerabilidades en el kit de desarrollo de software CODESYS V3, que permiten ataques de ejecución remota de código (RCE) y denegación de servicio (DoS).

3. **DETALLE:**

Más de 500 fabricantes de dispositivos utilizan el CODESYS V3 SDK para programar más de 1,000 modelos de PLC según el estándar IEC 61131-3, lo que permite a los usuarios desarrollar secuencias de automatización personalizadas.

El SDK también proporciona una interfaz de gestión de Windows y un simulador que permite a los usuarios probar su configuración y programación de PLC antes de implementarla en producción.

Las quince fallas en el CODESYS V3 SDK fueron descubiertas por investigadores de Microsoft, quienes las informaron a CODESYS en septiembre de 2022. El proveedor lanzó actualizaciones de seguridad para abordar los problemas identificados en abril de 2023.

Debido a la naturaleza de estos dispositivos, no se actualizan con frecuencia para solucionar problemas de seguridad, por lo que el equipo de seguridad de Microsoft publicó una publicación detallada para aumentar la conciencia sobre los riesgos y ayudar a acelerar el proceso de parcheo.

Las vulnerabilidades de CODESYS Microsoft examinó dos PLC de Schnieder Electric y WAGO que utilizan CODESYS V3 y descubrió 15 vulnerabilidades de alta gravedad (CVSS v3: 7.5 - 8.8).

Las fallas son:

- CVE-2022-47378
- CVE-2022-47379
- CVE-2022-47380
- CVE-2022-47381
- CVE-2022-47382
- CVE-2022-47383
- CVE-2022-47384
- CVE-2022-47385
- CVE-2022-47386
- CVE-2022-47387
- CVE 2022-47388
- CVE-2022-47389
- CVE-2022-47390
- CVE-2022-47392
- CVE-2022-47393

El problema principal se encuentra en el mecanismo de decodificación de etiquetas del SDK, específicamente en el hecho de que las etiquetas se copian en el búfer del dispositivo sin verificar su tamaño, lo que brinda a los atacantes la oportunidad de desbordar el búfer.

Estas etiquetas son portadoras de datos o estructuras de datos que proporcionan instrucciones cruciales para el funcionamiento del PLC.

El problema de desbordamiento del búfer no está aislado, ya que Microsoft lo encontró en 15 componentes del CODESYS V3 SDK, incluidos CMPTraceMgr, CMPapp, CMPDevice, CMPApp, CMPAppBP, CMPAppForce y CMPFileTransfer.

Aunque las fallas requieren autenticación para ser explotadas, Microsoft dice que este requisito se puede eludir usando CVE-2019-9013, otra falla que afecta a CODESYS V3 y expone las credenciales de usuario durante el transporte en forma de texto claro.

En 12 de los 15 casos, los analistas de Microsoft pudieron aprovechar la falla para lograr la ejecución remota de código en el PLC.

La advertencia de seguridad de CODESYS enumera los siguientes productos como afectados si ejecutan versiones anteriores a 3.5.19.0, independientemente de la configuración de hardware y sistema operativo:

- CODESYS Control RTE (SL)
- CODESYS Control RTE (para Beckhoff CX)
- SL CODESYS Control Win (SL)
- CODESYS Control Runtime System Toolkit
- CODESYS Safety SIL2 Runtime Toolkit
- CODESYS Safety SIL2 PSP CODESYS HMI (SL)
- CODESYS Development System V3
- CODESYS Development System V3 simulación en tiempo de ejecución

Además de lo anterior, los siguientes productos se ven afectados en versiones anteriores a 4.8.0.0:

- CODESYS Control for BeagleBone SL
- CODESYS Control for emPC-A/iMX6 SL
- CODESYS Control for IOT2000 SL
- CODESYS Control for Linux SL
- CODESYS Control for PFC100 SL
- CODESYS Control for PFC200 SL
- CODESYS Control for PLCnext SL
- CODESYS Control for Raspberry Pi SL
- CODESYS Control for WAGO Touch Panels 600 SL

4. RECOMENDACIONES

- Se recomienda a los administradores que actualicen a CODESYS V3 v3.5.19.0 lo antes posible, mientras que Microsoft también recomienda desconectar los PLC y otros dispositivos industriales críticos de Internet.

5. REFERENCIAS:

- Industrial PLCs worldwide impacted by CODESYS V3 RCE flaws (bleepingcomputer.com)

Vulnerabilidad alta en Armor PowerFlex de Rockwell Automation

Tipo de Ataque: Vulnerabilidad

Medio de Propagación: Internet

PRODUCTOS AFECTADOS:

- Armor PowerFlex: v1.003 - Rockwell

1. RESUMEN:

Se detecto una vulnerabilidad que permite a un atacante enviar una gran cantidad de comandos de red lo que provocaría que el producto genere un flujo de trafico de registro de eventos a una alta velocidad, resultando en una denegación de servicios.

2. DETALLE:

Se descubrió una vulnerabilidad en Armor PowerFlex cuando el producto envía comunicaciones al registro de eventos local. Actores de amenazas podrían explotar esta vulnerabilidad enviando una gran cantidad de comandos de red, lo que provocaría que el producto genere un flujo de tráfico de registros de eventos a una alta velocidad. Si se explota, el producto detendría las operaciones normales y se reiniciaría. El código de error debería ser borrado antes de reanudar las operaciones normales.

Se ha asignado CVE-2023-2423 a esta vulnerabilidad. Se ha calculado una puntuación base de CVSS v3 de 7.5; la cadena vectorial CVSS es (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

No se han reportado explotaciones públicas conocidas que apunten específicamente a estas vulnerabilidades hasta el momento.

3. RECOMENDACIONES:

Rockwell Automation recomienda a los usuarios aplicar las siguientes mitigaciones:

- Actualizar Armor PowerFlex a la versión v2.001 o posterior.
- Implementar las mejores prácticas de seguridad de Rockwell Automation.
- Para obtener más información, visitar el boletín de seguridad de Rockwell Automation.

CISA recomienda a los usuarios tomar medidas defensivas para minimizar el riesgo de explotación de esta vulnerabilidad. En particular, se debe:

- Minimizar la exposición de red para todos los dispositivos y sistemas de control, asegurándose de que no sean accesibles desde Internet.
- Colocar las redes de sistemas de control y dispositivos remotos detrás de firewalls y aislarlos de las redes empresariales.
- Utilizar métodos seguros, como redes privadas virtuales (VPNs), cuando se requiera acceso remoto, reconociendo que las VPN pueden tener vulnerabilidades y deben actualizarse a la versión más reciente disponible.
- CISA también recuerda realizar un análisis de impacto y evaluación de riesgos adecuados antes de implementar medidas defensivas.

4. REFERENCIAS:

- Rockwell Automation Armor PowerFlex | CISA
- Armor ™ PowerFlex ® Critical Fault Vulnerability (custhelp.com)