Alerta de Seguridad

Riesgo de vulnerabilidades IT y OT

Julio-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 marzo.

Alertas de Seguridad IT:

- Cl0p Ransomware usando MOVEit habría ganado US$ 100M en el ataque del 2Q de 2023
- Hackers chinos acceden al correo electrónico del embajador de EE.UU. en China
- Vulnerabilidad crítica en productos de Fortinet
- El Hacking a Microsoft Cloud expuso más que los correos electrónicos de Exchange y Outlook

Alertas de Seguridad OT/ICS:

- General Electric Cimplicity ha emitido parches para vulnerabilidades críticas que provendrían de ataques rusos a ICS
- CISA advierte sobre vulnerabilidades Críticas en equipos Honeywell, Siemens e Iagona

Cl0p Ransomware usando MOVEit habría ganado US$ 100M en el ataque del 2Q de 2023

Tipo de Ataque: Ransomware

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- MOVEit

2. RESUMEN:

Las investigaciones continúan sobre este ataque del que informamos en nuestro último boletín.

Según la empresa de recuperación de ransomware Coveware, el grupo Cl0p de ransomware podría haber ganado hasta $100 millones con el hackeo de MOVEit, que ha afectado a cientos de organizaciones. En el segundo trimestre de 2023, solo el 34% de las víctimas pagaron el rescate, la cifra más baja registrada. Aunque las probabilidades de pago son menores cuando los ataques involucran solo robo de datos sin encriptar archivos, el monto del rescate suele ser más alto. Coveware estima que, aunque el ataque de MOVEit puede afectar a más de 1,000 compañías directa e indirectamente, solo un pequeño porcentaje de las víctimas intentó negociar o considerar pagar el rescate. Aquellos que pagaron, lo hicieron en cantidades significativamente mayores que en campañas anteriores de Cl0p.

3. DETALLE:

Se cree que el grupo Cl0p podría haber ganado entre $75 y $100 millones solo con el hackeo de MOVEit, proveniente de un pequeño grupo de víctimas que accedió a pagar rescates muy altos. El grupo ha utilizado tácticas como establecer sitios web dedicados para algunas de las principales empresas objetivo, como EY y PwC, donde publican datos robados para presionar a las víctimas a pagar.

Se ha identificado a casi 400 víctimas del hackeo de MOVEit, incluidas organizaciones afectadas directa e indirectamente. Empresas importantes como BBC y British Airways también resultaron impactadas indirectamente a través de proveedores afectados. Por ejemplo, Zellis, una empresa de nómina y recursos humanos con sede en el Reino Unido fue atacada directamente, y otras compañías que utilizaban los servicios de Zellis, como BBC y British Airways, se vieron afectadas indirectamente.

PBI, una empresa que proporciona servicios de investigación para el sector de pensiones, seguros y finanzas, también fue víctima del hackeo, comprometiendo la información de varias organizaciones y millones de personas.

El ataque de MOVEit explotó una vulnerabilidad de día cero, lo que permitió a los ciberdelincuentes acceder a datos transferidos por organizaciones a través de la solución de transferencia de archivos administrados. Afortunadamente, muchas organizaciones han abordado rápidamente las vulnerabilidades de día cero y otros problemas descubiertos en MOVEit.

4. RECOMENDACIONES:

- Contar con un equipo ciberseguridad que esté atento a las vulnerabilidades de día cero que sean detectadas en las herramientas usadas por su organización.

5. REFERENCIAS:

- MOVEit Hack Could Earn Cybercriminals $100M as Number of Confirmed Victims Grows - SecurityWeek

Hackers chinos acceden al correo electrónico del embajador de EE.UU. en China

Tipo de Ataque: Hackeo

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**

- Cuentas de correo electrónico

2. **RESUMEN:**

Hackers chinos han accedido a las cuentas de correo electrónico del embajador de Estados Unidos en China, Nicholas Burns, y del subsecretario de Estado para Asia Oriental, Daniel Kritenbrink, como parte de una reciente campaña de recopilación de información.

3. **DETALLE:**

Esta noticia se suma al ciberataque chino revelado la semana pasada, donde también se infiltraron en los correos electrónicos de la secretaria de Comercio, Gina Raimondo. Funcionarios estadounidenses consideran que China es el adversario más avanzado de Estados Unidos en el ciberespacio y que tiene un programa de piratería más grande que todos los demás gobiernos combinados.

Los hackers violaron el sistema de correo electrónico no clasificado del gobierno de Estados Unidos, lo que llevó a creer que Beijing obtuvo información sobre la posición de Estados Unidos antes del viaje de alto perfil del secretario de Estado Antony Blinken a China en junio. Blinken planteó el tema en una reunión con el diplomático chino Wang Yi la semana pasada. Aunque se sospecha que los hackers chinos estaban detrás de esta actividad maliciosa, el Ministerio de Relaciones Exteriores de China acusó a Estados Unidos de realizar sus propias operaciones de piratería.

La piratería comenzó en mayo, y los hackers utilizaron una clave de inicio de sesión robada para acceder a las cuentas de correo electrónico. Tanto funcionarios del Departamento de Estado como de la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos están investigando la gravedad de la filtración y consideran que el equipo de hackers es sofisticado.

4. **REFERENCIAS:**

- Hackers chinos acceden al correo electrónico del embajador de EE.UU. en China (cnn.com)

Vulnerabilidad crítica en productos de Fortinet

Tipo de Ataque: Vulnerabilidades

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**

- FortiOS 7.0.0-7.0.10 y 7.2.0-7.2.3
- FortiProxy 7.0.0-7.0.9 y 7.2.0-7.2.2

2. **RESUMEN:**

El Centro Criptográfico Nacional (CCN-CERT) ha emitido una alerta sobre una vulnerabilidad crítica que afecta a los sistemas operativos FortiOS y FortiProxy de la empresa de ciberseguridad Fortinet.

3. **DETALLE:**

La vulnerabilidad detectada se trata de CVE-2023-33308, clasificada por la propia compañía como 9.8 en CVSS 3.1

Esta vulnerabilidad de desbordamiento basada en pila [CWE-124] en Fortinet FortiOS versión 7.0.0 a 7.0.10 y 7.2.0 a 7.2.3 y FortiProxy versión 7.0.0 a 7.0.9 y 7.2.0 a 7.2.2 permite a un atacante remoto no autenticado para ejecutar código o comando arbitrario a través de paquetes manipulados que alcanzan políticas de proxy o políticas de firewall con modo proxy junto con inspección profunda o completa de paquetes.

Hasta ahora, no se han reportado actividades maliciosas relacionadas con esta vulnerabilidad ni se han publicado pruebas de concepto que detallen los detalles de la falla. Sin embargo, dado que se considera crítica, es importante tomar medidas preventivas y actualizar los sistemas para evitar posibles ciberataques.

4. **RECOMENDACIONES:**
   - Fortinet ha lanzado una actualización de seguridad para solucionar el problema, y tanto la empresa como el CCN-CERT recomiendan a los usuarios y administradores de sistemas que actualicen a la nueva versión lo antes posible.
5. **REFERENCIAS:**

- https://www.welivesecurity.com/la-es/2022/06/08/follina-vulnerabilidad-critica-explotada-mediante-documentos-office/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

El Hacking a Microsoft Cloud expuso más que los correos electrónicos de Exchange y Outlook

Tipo de Ataque: Vulnerabilidad

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**

- Outlook, Exchange, SharePoint, Teams y OneDrive

2. **RESUMEN:**

Los investigadores de seguridad en la startup de nube Wiz advierten a las organizaciones que utilizan la plataforma M365 de Microsoft sobre una vulnerabilidad grave. La clave de seguridad de Microsoft robada permitió a los hackers chinos acceder a datos más allá de Exchange Online y Outlook.com.

3. **DETALLE:**

El equipo de investigación de Wiz encontró que la clave MSA comprometida podría haber permitido a los atacantes forjar tokens de acceso para múltiples tipos de aplicaciones de Azure Active Directory, incluidas aquellas que admiten la autenticación de cuentas personales, como SharePoint, Teams y OneDrive. Además, los hackers también podrían haber accedido a aplicaciones de clientes de Microsoft que admiten la función "iniciar sesión con Microsoft" y aplicaciones multiinquilino en ciertas condiciones.

Inicialmente, Microsoft solo había reconocido el impacto en Outlook.com y Exchange Online, pero la nueva investigación revela que el alcance de la vulnerabilidad es más amplio de lo pensado. Además, las organizaciones pueden tener dificultades para detectar el uso de tokens falsificados debido a la falta de registros cruciales relacionados con el proceso de verificación de tokens.

Aunque Microsoft ha revocado la clave comprometida, lo que significa que las aplicaciones de Azure Active Directory ya no aceptarán tokens falsificados, Wiz advierte que pueden persistir problemas si se establecieron sesiones previas con permisos de aplicaciones específicas.

4. **RECOMENDACIONES:**
   - Se recomienda a los clientes de Microsoft que actualicen urgentemente las implementaciones de Azure SDK a la última versión y aseguren que el caché de aplicaciones esté actualizado para mitigar el riesgo de uso de la clave comprometida por actores malintencionados.
5. **REFERENCIAS:**
   - Microsoft Cloud Hack Exposed More Than Exchange, Outlook Emails - SecurityWeek

General Electric Cimplicity ha emitido parches para vulnerabilidades críticas que provendrían de ataques rusos a ICS

Tipo de Ataque: Vulnerabilidad

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- Sistemas de control industriales

2. RESUMEN:

Recientemente, General Electric (GE) ha parcheado más de una docena de vulnerabilidades en su producto Cimplicity, que recuerdan a ataques a sistemas de control industrial (ICS) realizados por un notorio grupo de hackers rusos.

3. DETALLE:

La Agencia de Seguridad de Ciberseguridad e Infraestructura de EE. UU. (CISA) publicó recientemente un aviso para informar a los usuarios sobre las vulnerabilidades encontradas en la interfaz humano-máquina (HMI) y el sistema de adquisición y control de datos (SCADA) de Cimplicity de GE, que es utilizado por importantes organizaciones en todo el mundo, incluidos sectores de infraestructura crítica.

NVD califica la vulnerabilidad CVE-2023-3463 como crítica (9.8 en CVSS 3.1).

GE ha lanzado un parche y ha señalado: "La explotación solo es posible si un usuario autenticado con acceso local al sistema obtiene y abre un documento de una fuente maliciosa, por lo que una implementación segura y una gestión de acceso sólida por parte de los usuarios es esencial".

Michael Heinzl, el investigador de ciberseguridad de ICS que descubrió las vulnerabilidades dijo a SecurityWeek que, aunque solo se ha asignado un identificador CVE, en realidad hay un total de 14 vulnerabilidades de corrupción de memoria, que incluyen punteros no inicializados, lectura y escritura fuera de límites, uso después de liberar y desbordamiento de búfer basado en heap.

El investigador dijo que cada vulnerabilidad puede ser explotada para ejecución arbitraria de código al hacer que un usuario legítimo abra un archivo de proyecto .cim especialmente diseñado, y señaló que el ataque funciona en la configuración predeterminada del producto en todas las versiones.

Las últimas vulnerabilidades de GE Cimplicity son similares a los ataques realizados hace una década por un grupo de hackers rusos patrocinado por el estado, conocido como Sandworm, famoso por sus ataques disruptivos en el sector energético de Ucrania.

Trend Micro informó en 2014 que el grupo Sandworm había atacado a organizaciones que utilizan el producto Cimplicity y la operación involucraba el uso de archivos .cim como vectores de ataque.

CISA emitió una advertencia a las organizaciones en ese momento en relación con esos ataques. Su análisis, actualizado hasta 2021, mostró que los atacantes habían explotado una vulnerabilidad de Cimplicity rastreada como CVE-2014-0751 para "hacer que el servidor HMI ejecute un archivo .cim

malicioso [archivo de pantalla de Cimplicity] alojado en un servidor controlado por el atacante". En aquella ocasión, los atacantes utilizaron archivos.cim para desplegar el malware BlackEnergy.

4. RECOMENDACIONES:

- Actualizar los sistemas de GE con los parches de seguridad lanzados por la firma.

5. REFERENCIAS:

- Recently Patched GE Cimplicity Vulnerabilities Reminiscent of Russian ICS Attacks - SecurityWeek

CISA advierte sobre vulnerabilidades Críticas en equipos Honeywell, Siemens e Iagona

Tipo de Ataque: Vulnerabilidad

Medio de Propagación: Red, Internet

1. **PRODUCTOS AFECTADOS:**
   - Equipos Industriales
2. **RESUMEN:**

Diversas vulnerabilidades críticas para equipos industriales han sido publicadas por CISA (Cybersecurity & Infrastructure Security Agency)

3. **DETALLE:**

Honeywell Experion PKS, LX and PlantCruise

- Severidad: CVSS v3 9.8
- Atención: Explotable remotamente/ataque de baja complejidad
- Proveedor: Honeywell
- Equipo: Experion PKS, LX, and PlantCruise
- Vulnerabilidades: Heap-based Buffer Overflow, Stack-based Buffer Overflow, Out-of-bounds Write, Uncontrolled Resource Consumption, Improper Encoding or Escaping of Output, Deserialization of Untrusted Data, Improper Input Validation, Incorrect Comparison
- Riesgo: La explotación exitosa de estas vulnerabilidades podría causar una condición de denegación de servicio, permitir la escalada de privilegios o permitir la ejecución remota de código.

Siemens RUGGEDCOM ROX

- Severidad: CVSS v3 9.8
- Atención: Explotable de forma remota / complejidad de ataque baja
- Proveedor: Siemens
- Equipo: RUGGEDCOM ROX
- Vulnerabilidades: Transmisión en texto claro de información sensible, Inyección de comandos, Autenticación inadecuada, Desbordamiento de búfer clásico, Consumo no controlado de recursos, Validación incorrecta de certificados, Falsificación de petición entre sitios (CSRF), Validación incorrecta de entradas, Permisos predeterminados incorrectos, Script entre sitios (Cross-site Scripting), Fuerza de encriptación inadecuada, Uso de un algoritmo criptográfico roto o riesgoso.
- Riesgo: La explotación exitosa de estas vulnerabilidades podría permitir que un atacante envíe un paquete HTTP con formato incorrecto que cause que ciertas funciones fallen, logre un ataque de intermediario o la ejecución de código arbitrario.

Siemens SIMATIC CN 4100

- Severidad: CVSS v3 9.9
- Atención: Explotable de forma remota/baja complejidad de ataque
- Proveedor: Siemens
- Equipo: SIMATIC CN 4100
- Vulnerabilidades: control de acceso inadecuado, permisos predeterminados incorrectos
- Riesgo: La explotación exitosa de estas vulnerabilidades podría permitir a un atacante obtener una escalada de privilegios y eludir el aislamiento de la red.

Iagona ScrutisWeb

- Severidad: CVSS v3 10.0
- Atención: Explotable de forma remota/baja complejidad de ataque
- Vendedor: Iagona
- Equipo: ScrutisWeb
- Vulnerabilidades: cruce de ruta absoluta, omisión de autorización a través de clave controlada por el usuario, uso de clave criptográfica codificada, carga sin restricciones de archivos con tipo peligroso
- Riesgo: La explotación exitosa de estas vulnerabilidades podría permitir que un atacante cargue y ejecute archivos arbitrarios.

4. RECOMENDACIONES

- Actualizar los equipos mencionados a los últimos parches y actualizaciones de seguridad.

5. REFERENCIAS:

- Honeywell Experion PKS, LX and PlantCruise | CISA
- Siemens RUGGEDCOM ROX | CISA
- Siemens SIMATIC CN 4100 | CISA
- Iagona ScrutisWeb | CISA