Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Septiembre - 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 septiembre.

Alertas de Seguridad IT:

- Brecha de Datos Masiva en CMS Revela Vulnerabilidades Sistémicas en el Sector Salud de EE.UU.
- El error crítico de omisión de autenticación de Ivanti vTM ahora se explota en ataques
- Los paquetes Python convertidos en armas liberan puertas traseras PondRAT para Linux y MacOS

Alertas de Seguridad OT/ICS:

- Medidores automáticos de tanques utilizados en infraestructuras críticas plagadas de vulnerabilidades críticas
- El ciberataque a la planta de agua de Kansas obliga a cambiar a operaciones manuales

Brecha de Datos Masiva en CMS Revela Vulnerabilidades Sistémicas en el Sector Salud de EE.UU.

Tipo de Ataque: Ransomware (Cl0p)

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de gestión de datos y archivos (MOVEit Transfer)

2. **RESUMEN:**

La agencia federal Centros de Servicios de Medicare y Medicaid (CMS) ha informado que más de tres millones de beneficiarios de planes de salud vieron expuesta su información personal y de salud debido a los ataques MOVEit del ransomware Cl0p. Estos datos fueron robados tras una violación en la seguridad de Wisconsin Physicians Service (WPS), una empresa que administra servicios de Medicare.

3. **DETALLE:**

El ciberataque afectó a CMS, una agencia que administra los programas de atención médica más grandes de Estados Unidos, como Medicare, Medicaid y CHIP. CMS reportó el incidente a través de un comunicado de prensa el 6 de septiembre, donde notificó que 946,801 personas con Medicare fueron afectadas directamente. No obstante, el número total de personas afectadas asciende a 3.112.815, según el portal de violaciones de datos del Departamento de Salud y Servicios Humanos de EEUU (HHS).

El ataque se produjo mediante una vulnerabilidad en MOVEit Transfer, un software utilizado por WPS para gestionar datos. Aunque WPS aplicó los parches de seguridad en junio de 2023, una revisión realizada en mayo de 2024 reveló que los piratas informáticos habían accedido a la red antes de que se implementaran dichas actualizaciones, lo que permitió la exfiltración de archivos sensibles.

CMS ha tomado medidas inmediatas para notificar a los afectados y coordinar con WPS, que ha iniciado un proceso de investigación y refuerzo de seguridad. El ataque Cl0p pone de relieve la vulnerabilidad de los sistemas de gestión de datos y la importancia de implementar actualizaciones de seguridad de manera proactiva y oportuna.

4. **RECOMENDACIONES:**
   - Realizar una auditoría exhaustiva de seguridad para identificar y parchar vulnerabilidades en los sistemas de gestión de datos.
   - Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para garantizar una mejora continua en la ciberseguridad.
   - Fortalecer las medidas de ciberseguridad a nivel federal y estatal, especialmente en el sector de la salud, para prevenir futuros incidentes.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/healthcare/us-govt-agency-cms-says-data-breach-impacted-31-million-people/

El error crítico de omisión de autenticación de Ivanti vTM ahora se explota en ataques

Tipo de Ataque: Desconocido

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Dispositivos Virtual Traffic Manager (vTM) de Ivanti
2. **RESUMEN:**

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) ha etiquetado una nueva vulnerabilidad crítica en los dispositivos Virtual Traffic Manager (vTM) de Ivanti, que permite a atacantes remotos crear usuarios administradores no autorizados. La falla, identificada como CVE-2024-7593, se está explotando activamente, subrayando la necesidad urgente de reforzar la seguridad en infraestructuras que dependen de estos dispositivos para la gestión de tráfico y servicios críticos.

3. **DETALLE**

La vulnerabilidad CVE-2024-7593 fue descubierta en el software Virtual Traffic Manager (vTM) de Ivanti, un controlador de entrega de aplicaciones que proporciona equilibrio de carga y gestión de tráfico para servicios críticos. Esta falla de omisión de autenticación se debe a la implementación incorrecta de un algoritmo de autenticación, permitiendo que atacantes remotos no autenticados eludan la seguridad y accedan a los paneles de administración expuestos a Internet.

Ivanti lanzó un parche el 13 de agosto de 2024, después de que el código de explotación de prueba de concepto (PoC) se hiciera público. Sin embargo, aún no han confirmado la explotación activa en el aviso de seguridad. No obstante, CISA agregó esta vulnerabilidad a su catálogo de fallas explotadas activamente, lo que exige a las agencias federales proteger sus dispositivos vulnerables antes del 15 de octubre de 2024.

La explotación exitosa de esta vulnerabilidad permite a los atacantes crear usuarios administradores no autorizados, lo que podría poner en riesgo la infraestructura crítica de las organizaciones. Ivanti ha recomendado a los administradores que verifiquen los registros de auditoría para detectar la creación de nuevos usuarios 'usuario1' o 'usuario2' como indicio de un compromiso potencial. También se aconseja restringir el acceso a la interfaz de administración vTM limitándola a redes internas o direcciones IP privadas, reduciendo así la superficie de ataque.

Ivanti ha sido un objetivo frecuente de ciberataques en los últimos meses, con vulnerabilidades en sus dispositivos VPN y puertas de enlace ICS explotadas en múltiples incidentes. En respuesta, la compañía ha mejorado sus capacidades internas de escaneo y pruebas, acelerando su proceso de divulgación responsable para abordar problemas de seguridad con mayor rapidez.

4. RECOMENDACIONES:

- Aplicar de inmediato los parches de seguridad proporcionados por Ivanti para corregir la vulnerabilidad CVE-2024-7593.
- Restringir el acceso a las interfaces de administración vTM a redes internas o direcciones IP privadas.
- Revisar los registros de auditoría para detectar actividades sospechosas, como la creación de nuevos usuarios no autorizados.
- Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para garantizar una mejora continua en la protección de infraestructuras críticas.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/critical-ivanti-vtm-auth-bypass-bug-now-exploited-in-attacks/

Los paquetes Python convertidos en armas liberan puertas traseras PondRAT para Linux y MacOS

Tipo de Ataque: Desconocido

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**

- Sistemas Linux y macOS
- Paquetes Python (real-ids, colourtxt, beautifultext, minisound)

1. **RESUMEN:**

El grupo de amenazas norcoreano Gleaming Pisces ha lanzado una campaña de ataques cibernéticos dirigidos a la industria de las criptomonedas mediante la infiltración de software comercial falso y la distribución de malware, como PondRAT. Este malware afecta tanto a sistemas Linux como macOS y se ha detectado que comparte similitudes de código con otras amenazas previamente atribuidas al mismo grupo, como AppleJeus y POOLRAT.

2. **DETALLE:**

Desde 2018, Gleaming Pisces ha estado activo en el ámbito de la ciberdelincuencia, enfocándose principalmente en la industria de las criptomonedas. Recientemente, se ha vinculado al grupo con una campaña que utiliza paquetes Python envenenados subidos a PyPI, entre ellos real-ids, colourtxt, beautifultext y minisound. Estos paquetes ejecutaban código malicioso que desplegaba PondRAT, un troyano de acceso remoto (RAT) para Linux.

PondRAT comparte una base de código con malware previamente identificado, como POOLRAT, lo que indica una clara conexión en el modus operandi de Gleaming Pisces. Un análisis de VIPYR reveló que las variantes de PondRAT en macOS y Linux no solo comparten nombres de funciones idénticas, sino que también utilizan una clave de cifrado común. Ambas versiones del malware exhiben similitudes estructurales que sugieren que la variante de Linux es una adaptación de la versión macOS.

La investigación de la Unidad 42 confirmó que la variante "os_helper" de macOS, parte de la campaña de paquetes Python envenenados, utilizaba la misma infraestructura C2 que su contraparte en Linux. Estas actividades también fueron vinculadas a la campaña AppleJeus, consolidando aún más la atribución a Gleaming Pisces.

A pesar de que PondRAT es una versión simplificada de POOLRAT, aún representa una amenaza considerable para las organizaciones debido a su capacidad para explotar paquetes legítimos de Python, lo que le permite eludir los mecanismos de detección convencionales y comprometer redes de manera generalizada. Gleaming Pisces continúa adaptando su malware, aprovechando la infraestructura compartida y los avances en técnicas de evasión para expandir sus campañas cibernéticas.

3. RECOMENDACIONES

- Analizar y monitorizar los paquetes Python instalados en los sistemas para detectar actividades sospechosas.
- Implementar soluciones de seguridad que bloqueen el acceso a repositorios de software no confiables.
- Realizar auditorías de seguridad periódicas en infraestructuras críticas, especialmente aquellas que operan con sistemas Linux y macOS.
- Asegurarse de que los sistemas cuenten con las últimas actualizaciones y parches de seguridad para mitigar vulnerabilidades explotadas por malware como PondRAT.
- Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para mejorar la resiliencia cibernética de la organización.

4. REFERENCIAS:

- https://cyberpress.org/python-packages-drop-pondrat-linux-and-macos/

Medidores automáticos de tanques utilizados en infraestructuras críticas plagadas de vulnerabilidades críticas

Tipo de Ataque: Desconocido

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- Maglink LX y LX4
- OPW SiteSentinel
- Proteus OEL8000
- Alisonic Sibylla
- Franklin TS-550

2. RESUMEN:

Casi una década después de las primeras advertencias, los sistemas de medición automática de tanques (ATG) siguen expuestos a ciberataques. Estos dispositivos, que monitorean parámetros como el volumen y la temperatura de los tanques de almacenamiento en infraestructuras críticas, presentan múltiples vulnerabilidades que pueden ser explotadas de forma remota.

3. DETALLE:

Un análisis de Bitsight reveló 10 vulnerabilidades críticas en sistemas ATG de cinco proveedores. Entre las fallas más graves están la omisión de autenticación, credenciales codificadas y ejecución de comandos del sistema operativo. Estos dispositivos se utilizan en estaciones de servicio, aeropuertos, hospitales y plantas de energía, exponiendo infraestructuras críticas a potenciales ataques. En algunos casos, los atacantes podrían provocar daños físicos a los sistemas o acceder a redes internas.

El estudio mostró que miles de estos dispositivos están expuestos a nivel mundial, particularmente en EE.UU. y Europa. Bitsight también advirtió sobre la falta de mejoras en la exposición de estos sistemas entre junio y septiembre, a pesar de las notificaciones enviadas a los proveedores afectados a través de la agencia de ciberseguridad estadounidense CISA.

4. RECOMENDACIONES:

- Evaluar la seguridad de los sistemas ATG y aplicar los parches necesarios.
- Implementar un Sistema de Gestión de Seguridad de Información (SGSI) para garantizar mejoras continuas en ciberseguridad.

5. REFERENCIAS:

- https://www.securityweek.com/automatic-tank-gauges-used-in-critical-infrastructure-plagued-by-critical-vulnerabilities/

El ciberataque a la planta de agua de Kansas obliga a cambiar a operaciones manuales

Tipo de Ataque: Desconocido

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- Instalaciones de tratamiento de agua (Sistemas ICS)

2. RESUMEN:

Arkansas City, en Kansas, fue víctima de un ciberataque que obligó a sus instalaciones de tratamiento de agua a operar manualmente. A pesar del incidente, el suministro de agua no fue interrumpido, y las autoridades han asegurado que es seguro para el consumo. La situación está siendo investigada por el FBI y el Departamento de Seguridad Nacional.

3. DETALLE:

El ciberataque contra Arkansas City fue detectado el domingo por la mañana, lo que llevó a los funcionarios a implementar operaciones manuales en la planta de tratamiento de agua como medida preventiva. Randy Frazer, administrador de la ciudad, aseguró que el suministro de agua sigue siendo seguro y que las operaciones no se han visto afectadas de manera significativa. Sin embargo, se advirtió a los residentes que podrían experimentar baja presión de agua temporalmente.

El incidente se produjo apenas dos días después de una advertencia emitida por el WaterISAC sobre posibles ataques dirigidos al sector del agua por actores de amenazas vinculados a Rusia. La Agencia de Protección Ambiental de EE.UU. también había emitido recientemente una guía para ayudar a los operadores de sistemas de agua a mejorar sus prácticas de ciberseguridad, lo que pone de manifiesto la creciente preocupación por la vulnerabilidad de las infraestructuras críticas en EE.UU.

En el pasado, los sistemas de agua y aguas residuales han sido blanco de ataques cibernéticos, incluidos ransomware y otros incidentes que comprometieron su operación. Estos eventos resaltan la necesidad de mayor inversión en ciberseguridad para proteger este sector crítico.

4. RECOMENDACIONES:

- Realizar una evaluación de ciberseguridad para sistemas de agua y aguas residuales.
- Implementar medidas de protección avanzadas, incluyendo un Sistema de Gestión de Seguridad de Información (SGSI).
- Monitorear y actualizar continuamente los sistemas ICS para evitar ataques futuros.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/kansas-water-plant-cyberattack-forces-switch-to-manual-operations/