Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Enero - 2024

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 Enero.

Alertas de Seguridad IT:

- Un millón de sitios web afectado por vulnerabilidad en plugin de base de datos de Wordpress.
- Ataque de Ransomware afecta al gigante de leasing de aviación, AerCap.
- Cibercriminales rusos de “Midnight Blizzard” vulneran cuenta de correos corporativos de Microsoft y HPE

Alertas de Seguridad OT/ICS:

- Ciberataque a compañías de servicios de agua en EEUU y Reino Unido
- Siemens y Schneider Electric lanzan los primeros avisos de parches de ICS de 2024.
- Vulnerabilidades descubiertas en Rapid SCADA por el equipo de Claroty

Un millón de sitios web afectado por vulnerabilidad en plugin de base de datos de Wordpress

Tipo de Ataque: Vulnerabilidades.

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS**
   - Plugin de WordPress: “Better Search Replace”
2. **RESUMEN:**

Un plugin de WordPress llamado "Better Search Replace" con más de 1 millón de instalaciones activas tiene una vulnerabilidad crítica que permite a los hackers tomar el control de los sitios web.

3. **DETALLE:**

Better Search Replace es un plugin de WordPress con más de un millón de instalaciones que ayuda con las operaciones de búsqueda y reemplazo en bases de datos al mover sitios web a nuevos dominios o servidores.

Los administradores pueden usarlo para buscar y reemplazar texto específico en la base de datos o manejar datos serializados, y proporciona opciones de reemplazo selectivo, soporte para WordPress Multisite, y también incluye una opción de "Dry Run" para asegurarse de que todo funciona bien.

El proveedor del plugin, WP Engine, lanzó la versión 1.4.5 la semana pasada para solucionar una vulnerabilidad de inyección de objetos PHP de severidad crítica rastreada como CVE-2023-6933. La cual hasta la fecha tiene un estado reservado en cve.org.

El problema de seguridad se deriva de la deserialización de entradas no confiables y permite a los atacantes no autenticados inyectar un objeto PHP. La explotación exitosa podría conducir a la ejecución de código, acceso a datos sensibles, manipulación o eliminación de archivos, y la activación de una condición de denegación de servicio de bucle infinito.

La descripción de la falla en el rastreador de Wordfence indica que Better Search Replace no es directamente vulnerable, pero puede ser explotado para ejecutar código, recuperar datos sensibles o eliminar archivos si otro plugin o tema en el mismo sitio contiene la cadena de Programación Orientada a Propiedades (POP).

La explotabilidad de las vulnerabilidades de inyección de objetos PHP a menudo depende de la presencia de una cadena POP adecuada que puede ser activada por el objeto inyectado para realizar acciones maliciosas.

Los hackers han aprovechado la oportunidad para explotar la vulnerabilidad ya que la firma de seguridad de WordPress Wordfence informa que ha bloqueado más de 2.500 ataques dirigidos a CVE-2023-6933 en sus clientes en solo 24 horas.

4. **RECOMENDACIONES**
   - Desactivar el plugin de WordPress hasta tener una actualización que parche esta vulnerabilidad.

- Contar con un MFA (Multiple Factor de Autentificación) para evitar que externo ingresen a las cuentas de administrador.
- Cambiar el dominio predeterminado de la ruta de acceso de usuarios.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/hackers-target-wordpress-database-plugin-active-on-1-million-sites/

Ataque de Ransomware afecta al gigante de leasing de aviación AerCap.

Tipo de Ataque: Ransomware.

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Base de datos
2. **RESUMEN:**

El pasado 17 de enero, AerCap, el gigante de leasing aéreo fue víctima de un ataque de ransomware, pero asegura haber tomado el control de la situación y no haber sufrido pérdidas financieras. Sin embargo, el grupo atacante amenaza con filtrar datos robados si no se paga un rescate. Las autoridades investigan el incidente.

3. **DETALLE:**

El gigante del leasing de aviones, AerCap, ha confirmado ser víctima de un ataque de ransomware después de que una nueva banda cibercriminal se atribuyera la responsabilidad. La intrusión ocurrió el 17 de enero, según informó la compañía en un documento presentado ante la Comisión de Bolsa y Valores de Estados Unidos (SEC).

"Mantenemos control total sobre todos nuestros sistemas informáticos y hasta la fecha no hemos sufrido ninguna pérdida financiera relacionada con este incidente", confirmó AerCap a la SEC.

Si bien la compañía no reveló detalles sobre los atacantes, un grupo emergente de ransomware llamado "Slug" ha asumido la responsabilidad del ataque, listando a AerCap en su sitio web de filtraciones.

Slug afirma haber robado aproximadamente un terabyte de datos de la empresa, amenazando con filtrar la información progresivamente a menos que se pague un rescate. El grupo asegura que, en dos semanas, todos los datos robados serán publicados públicamente.

Por el momento, el sitio web de filtraciones de Slug solo menciona a AerCap como víctima.

4. **RECOMENDACIONES**
   - Sensibilizar al recurso humano de su organización para que evite descargar aplicaciones sospechosas.
   - Controlar la descarga de aplicaciones y software para asegurar que sea legítimo. Además, controlar los permisos que tienen los usuarios sobre las aplicaciones basado en el concepto de Zero Trust.

5. **REFERENCIAS:**
   - https://www.securityweek.com/aircraft-lessor-aercap-confirms-ransomware-attack/

Cibercriminales rusos de “Midnight Blizzard” vulneran cuentas de correos corporativos de Microsoft y HPE

Tipo de Ataque: **Password Spraying.**

Medio de Propagación: **Internet**

1. **PRODUCTOS AFECTADOS:**
   - Correos Corporativos
2. **RESUMEN:**

Microsoft y HPE confirmaron una intrusión por el grupo ruso "Midnight Blizzard". El ataque a las cuentas de correo corporativo inició en noviembre de 2023 y fue detectado el 12 de enero de 2024. Se accedió a cuentas de líderes sénior y roles legales y de ciberseguridad. La respuesta inmediata incluyó investigación y mitigación; no se encontraron pruebas de acceso a sistemas clave.

3. **DETALLE:**

Microsoft informó en una publicación de blog que el pasado 12 de enero su equipo de seguridad detectó un ataque patrocinado por un Estado, identificado como el grupo de hackers rusos, que comenzó en noviembre de 2023.

La empresa activó de inmediato su proceso de respuesta para investigar, interrumpir la actividad maliciosa, mitigar el ataque y bloquear el acceso adicional al actor de la amenaza. Hasta ahora, no hay evidencia de que el actor de la amenaza haya accedido a los entornos de los clientes, sistemas de producción, código fuente o sistemas de inteligencia artificial. La empresa notificará a los clientes si se requiere alguna acción adicional.

Los cibercriminales emplearon un ataque de password spray (pulverización de contraseñas) para comprometer una cuenta heredada de un inquilino de prueba, que no era de producción. Posteriormente, utilizaron los permisos obtenidos para acceder a cuentas de correo electrónico, principalmente en búsqueda de información relacionada con "Midnight Blizzard".

4. **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 multifactor.

5. REFERENCIAS:

- https://www.itmastersmag.com/ciberseguridad/microsoft-y-hpe-reconocen-vulneracion-por-parte-de-los-rusos-midnight-blizzard/
- https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/

Ciberataque a compañías de servicios de agua en EEUU y Reino Unido

Tipo de Ataque: Ransomware

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - ICS
   - Servidores
2. **RESUMEN:**

Veolia North America en Estados Unidos y Southern Water en el Reino Unido fueron blanco de ataques de ransomware, comprometiendo la seguridad de estas importantes empresas de agua. Veolia confirmó la intrusión en su división Municipal Water, desactivando sistemas afectados, mientras que Southern Water enfrenta amenazas de hacer pública información robada si no se paga un rescate.

3. **DETALLE:**

Veolia North America, la compañía de agua más grande del mundo según su descripción, que proporciona servicios de agua y aguas residuales a decenas de millones de personas, anunció en su sitio web que su división Municipal Water fue afectada por ransomware la semana pasada. En respuesta al incidente, la empresa desactivó los sistemas y servidores específicos, lo que interrumpió los sistemas de pago de facturas en línea. Veolia aseguró que el incidente parece haberse limitado a los sistemas internos de Veolia North America y no hay evidencia de que haya afectado las operaciones de tratamiento de agua o aguas residuales.

Southern Water en el Reino Unido también fue objetivo de un grupo de ransomware. Esta empresa, que proporciona servicios de agua a 2.5 millones de clientes y servicios de aguas residuales a 4.7 millones en el sur de Inglaterra, confirmó la detección de actividad sospechosa en sus sistemas y ha iniciado una investigación. El grupo de ransomware Black Basta afirmó en su sitio de filtraciones haber robado 750 GB de archivos de Southern Water, incluyendo información personal y documentos corporativos. Los ciberdelincuentes amenazan con hacer pública la información robada en cinco días si no se paga un rescate.

4. **RECOMENDACIONES:**
   - Identificar cualquier sistema de control industrial desplegado por su organización y/o sus socios comerciales externos, y evaluar rápidamente la seguridad de estos sistemas.
   - Emplear salvaguardias como cortafuegos para protegerse contra el acceso no autorizado a sus sistemas de control industrial.
5. **REFERENCIAS:**
   - https://www.securityweek.com/major-us-uk-water-companies-hit-by-ransomware/

Siemens y Schneider Electric lanzan los primeros avisos de parches de ICS de 2024.

Tipo de Ataque: Vulnerabilidades

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Redfish de MaxView Storage Manager
   - Simatic CN 4100
   - Solid Edge 2023
   - Teamcenter Visualization
   - JT2Go de Siemens
   - Spectrum Power 7
   - Sicam A8000
   - Easergy Studio
2. **RESUMEN:**

En el primer martes de actualizaciones de seguridad de 2024, destacadas corporaciones industriales como Siemens y Schneider Electric han lanzado importantes revisiones, abordando un total de siete nuevos informes y resolviendo 22 vulnerabilidades.

3. **DETALLE:**

Siemens ha difundido seis nuevos informes, siendo el más crítico el vinculado a una vulnerabilidad en los IPCs Simatic. Con una puntuación CVSS de 10, la vulnerabilidad afecta al componente servidor Redfish de MaxView Storage Manager. Se aconseja a los usuarios de MaxView instalar el parche proporcionado por Microchip para reducir el riesgo.

Adicionalmente, Siemens ha informado sobre vulnerabilidades críticas y de alta gravedad en Simatic CN 4100 que podrían permitir a los atacantes tomar control remoto de los dispositivos.

La empresa también ha abordado una docena de vulnerabilidades en Solid Edge 2023, relacionadas con un método de ataque que utiliza archivos PAR. Estos podrían permitir a los atacantes ejecutar código arbitrario al convencer a la víctima para que abra archivos especialmente diseñados.

Se han corregido también agujeros de seguridad en el procesamiento de archivos CGM en los productos Teamcenter Visualization y JT2Go de Siemens.

Adicionalmente, Siemens ha emitido un parche para una vulnerabilidad en Spectrum Power 7 que, aunque requiere acceso local con privilegios de administrador para su explotación, podría permitir la inyección de código arbitrario y acceso de root al sistema.

Una vulnerabilidad de gravedad media en los dispositivos Sicam A8000 también ha sido parcheada, evitando que atacantes autenticados inyecten comandos con privilegios de root durante el arranque.

Por su parte, Schneider Electric ha publicado un único informe para informar a los clientes sobre una vulnerabilidad de alta gravedad en Easergy Studio. Esta podría permitir que un atacante con una cuenta de nivel de usuario obtenga mayores privilegios al proporcionar un objeto serializado perjudicial.

4. RECOMENDACIONES:

- Aplicar de manera urgente los parches de seguridad de los fabricantes.

5. REFERENCIAS:

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

Vulnerabilidades descubiertas en Rapid SCADA por el equipo de Claroty

Tipo de Ataque: Vulnerabilidad

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Rapid SCADA: Version 5.8.4 y anteriores.
2. **RESUMEN:**

La plataforma de automatización industrial de código abierto Rapid SCADA se ve afectada por varias vulnerabilidades que podrían permitir a los hackers acceder a sistemas industriales sensibles, pero las fallas siguen sin parches. La agencia de ciberseguridad de EE. UU., CISA, emitió un aviso la semana pasada, informando sobre siete vulnerabilidades descubiertas por investigadores de Claroty en Rapid SCADA.

3. **DETALLE:**

Rapid SCADA es promocionado como una solución ideal para el desarrollo de sistemas de monitoreo y control, especialmente en ámbitos como la automatización industrial, sistemas IoT, contabilidad de energía y control de procesos. Sin embargo, estas vulnerabilidades, catalogadas como críticas y de alta severidad, según el aviso de CISA, plantean riesgos significativos para la seguridad.

Entre las vulnerabilidades identificadas se incluyen:

Categoría	Impacto	CVSS base score	CVSS vector	CVE Numbers
Improper limitation of a pathname to a restricted directory ('path traversal') CWE-22	Suministrar un archivo de configuración malicioso para ejecución remota de código.	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	CVE-2024-21852
Relative path traversal CWE-23	Al agregar caracteres de recorrido de ruta al nombre del archivo cuando se usa un comando específico, un atacante puede leer archivos arbitrarios del sistema.	6.5	CVSS:3.1 /AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	CVE-2024-22096
Local privilege escalation through incorrect permission assignment for critical resource CWE-732	Debido a una configuración incorrecta de permisos, cualquier usuario autenticado en el	7.8	CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	CVE-2024-22016

	servidor puede escribir directamente en el directorio de SCADA. Esto puede permitir una escalada de privilegios.			
Url redirection to untrusted site ('open redirect') CWE-601	El producto afectado puede permitir redireccionamientos abiertos a través de la página de inicio de sesión. Esto puede redirigir a los usuarios a páginas web maliciosas.	5.4	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:L	CVE-2024-21794
Use of hard-coded credentials CWE-798	El producto afectado utiliza credenciales codificadas, lo que puede permitir que un atacante se conecte a un puerto específico.	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVE-2024-21764
Plaintext storage of a password CWE-256	El producto afectado almacena credenciales en texto plano en varios lugares. Esto puede permitir que un atacante con acceso local los vea.	6.2	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	CVE-2024-21869
Generation of error message containing sensitive information CWE-209	El producto afectado responde con un mensaje de error que contiene datos confidenciales si recibe una solicitud específica con formato incorrecto.	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	CVE-2024-21866

A pesar de que los investigadores notificaron a los desarrolladores sobre estas vulnerabilidades en julio de 2023, aún no se han lanzado parches para corregir las fallas. Además, los intentos de CISA y Claroty para contactar a los desarrolladores no han tenido éxito, y estos tampoco han respondido a las solicitudes de comentarios.

Noam Moshe, investigador de vulnerabilidades en Claroty, destaca que Rapid SCADA se utiliza en diversos campos en el actual panorama de tecnología operativa, siendo una opción popular para empresas pequeñas y medianas debido a su naturaleza de código abierto y gratuita.

4. RECOMENDACIONES:

- Eliminar cualquier sistema de control industrial de la Internet pública.
- Emplear salvaguardias como cortafuegos para protegerse contra el acceso no autorizado a sus sistemas de control industrial.

5. REFERENCIAS:

- https://www.securityweek.com/unpatched-rapid-scada-vulnerabilities-could-expose-industrial-organizations-to-attacks/
- https://www.cisa.gov/news-events/ics-advisories/icsa-24-011-03