Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Noviembre - 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 Octubre.

Alertas de Seguridad IT:

- Tres vulnerabilidades críticas exponen los datos de usuarios de ownCloud
- Adobe libera actualizaciones de seguridad para Coldfusion
- Temu apuesta por la Ciberseguridad y se suma al programa de recompensas de HackerOne

Alertas de Seguridad OT/ICS:

- Ciberataque a camiones autónomos paraliza División Minera Gabriela Mistral de CODELCO
- CISA está respondiendo a la explotación activa de PLCs Unitronics

Tres vulnerabilidades críticas exponen los datos de usuarios de ownCloud

Tipo de Ataque: Vulnerabilidades.

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS**
   - ownCloud desde 10.6.0 hasta 10.13.0.
2. **RESUMEN:**

Tres vulnerabilidades críticas en el software de intercambio de archivos de código abierto ownCloud, que podrían ser explotadas para revelar información sensible y modificar archivos. Las vulnerabilidades son las siguientes:

3. **DETALLE:**

Entre las vulnerabilidades publicadas se encuentran del tipo críticas e importantes:

Categoría	Impacto	Severidad	CVSS base score	CVSS vector	CVE Numbers
No categorized	Divulgación de credenciales y configuración sensibles	Critical	10	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	CVE-2023-49103
Improper Authentication (CWE-287)	Bypass de autenticación de la API WebDAV	Critical	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVE-2023-49105
URL Redirection to Untrusted Site ('Open Redirect') (CWE-601)	Bypass de validación de subdominio	Critical	9.0	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N	CVE-2023-49104

La primera vulnerabilidad revela detalles de configuración del entorno PHP cuando se accede a una URL proporcionada por la aplicación 'graphapi', incluyendo datos sensibles en implementaciones contenerizadas, como contraseñas de administrador, credenciales del servidor de correo y claves de licencia. La solución recomendada por ownCloud es eliminar un archivo específico y desactivar la función 'phpinfo', además de cambiar contraseñas y claves.

La segunda vulnerabilidad permite el acceso, modificación o eliminación de cualquier archivo sin autenticación si se conoce el nombre de usuario de la víctima y esta no tiene configurada una clave de firma, que es el comportamiento predeterminado.

La tercera vulnerabilidad implica un control de acceso incorrecto que permite a un atacante redirigir callbacks a un dominio controlado por el atacante.

Para estas últimas 2 vulnerabilidades, ownCloud sugiere medidas correctivas, como fortalecer el código de validación en la aplicación oauth2 y desactivar la opción "Permitir subdominios" como solución temporal.

Además, se informa sobre un exploit de prueba de concepto para una vulnerabilidad crítica de ejecución remota de código en el software CrushFTP. Aunque esta vulnerabilidad ha sido corregida en la versión 10.5.2 de CrushFTP, se destaca su gravedad al permitir a un atacante no autenticado acceder a archivos, ejecutar programas arbitrarios y obtener contraseñas en texto plano.

La vulnerabilidad CVE-2023-49103 de ownCloud está siendo activamente explotada, según informes, con observaciones de explotación masiva desde el 25 de noviembre. Expertos señalan que los ataques contra ownCloud no son infrecuentes, siendo muchos de ellos intentos de aprovechar vulnerabilidades antiguas o contraseñas débiles**.**

4. **RECOMENDACIONES**
   - Validar si existen usuarios activos dentro de la organización que utilicen el software comprometido.
   - Seguir las recomendaciones del fabricante para evitar ser afectados por estas vulnerabilidades.
   - Realizar el análisis de las máquinas y actualizar el software a la versión más reciente.
5. **REFERENCIAS:**
   - https://thehackernews.com/2023/11/warning-3-critical-vulnerabilities.html
   - https://owncloud.com/security

Adobe libera actualizaciones de seguridad para Coldfusion

Tipo de Ataque: Vulnerabilidades.

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - ColdFusion 2021 y 2023
2. **RESUMEN:**

El 14 de noviembre de 2023, Adobe lanzó actualizaciones de seguridad para abordar vulnerabilidades que afectan al software no parcheado de ColdFusion. La explotación de algunas de estas vulnerabilidades podría permitir a un actor cibernético malicioso tomar el control de un sistema afectado.

3. **DETALLE:**

Entre las vulnerabilidades publicadas se encuentran del tipo críticas e importantes:

Categoría	Impacto	Severidad	CVSS base score	CVSS vector	CVE Numbers
Deserialization of Untrusted Data (CWE-502)	Ejecución de código arbitrario	Critical	9.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	CVE-2023-44350
Improper Access Control (CWE-284)	Bypass de controles de seguridad	Critical	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	CVE-2023-26347
Deserialization of Untrusted Data (CWE-502)	Ejecución de código arbitrario	Critical	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVE-2023-44351
Cross-site Scripting (Reflected XSS) (CWE-79)	Ejecución de código arbitrario	Important	6.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	CVE-2023-44352
Deserialization of Untrusted Data (CWE-502)	Ejecución de código arbitrario	Important	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	CVE-2023-44353

RECOMENDACIONES

- Aplicar las actualizaciones recomendadas en APSB23-52.
- Seguir las recomendaciones de Adobe sobre la protección de ColdFusion.
- Consultar las guías de seguridad ColdFusion 2023 y ColdFusion 2021.
- Considerar agregar un filtro de firewall de aplicaciones web (WAF) para CFIDE para usuarios externos.
- Evaluar el uso de los Playbooks de Respuesta a Incidentes y Vulnerabilidades de Ciberseguridad de CISA para pasos adicionales y acciones concretas.

4. **REFERENCIAS:**
   - Adobe Security Bulletin
   - Adobe Releases Security Updates for ColdFusion | CISA

Temu apuesta por la Ciberseguridad y se suma al programa de recompensas de HackerOne

1. RESUMEN:

Temu, una destacada aplicación global de compras, ha anunciado su asociación con HackerOne, una agencia líder en ciberseguridad, a través de su programa de recompensas por errores de seguridad, también conocido como "bug bounty". Este programa tiene como objetivo identificar y mitigar posibles vulnerabilidades en la plataforma de Temu, uniéndose a empresas destacadas como Amazon, Google, Tesla y Meta que ya participan en esta iniciativa.

2. DETALLE:

El programa "bug bounty" permite a las empresas colaborar con hackers éticos para mejorar la seguridad de sus sistemas. A pesar de ser una incorporación reciente a esta iniciativa, Temu ha tomado medidas significativas para fortalecer su postura en ciberseguridad. Recientemente, la empresa emprendió acciones legales contra sitios web que infringían su marca y participaban en actividades de phishing y fraude, demostrando un claro compromiso con la protección de sus usuarios.

Un portavoz de Temu destacó: "En Temu, la privacidad y la seguridad son aspectos fundamentales de nuestra plataforma. Nuestra prioridad principal es ganar y mantener la confianza de nuestros usuarios, por lo que nos adherimos a los estándares más rigurosos en materia de seguridad y privacidad". Además, añadió: "Estamos comprometidos en colaborar con servicios de seguridad para identificar y resolver vulnerabilidades, aumentar la transparencia en las pruebas de seguridad y garantizar la absoluta fiabilidad tanto para nuestras empresas como para nuestros clientes".

El programa de recompensas por errores de Temu ofrece pagos que varían desde $30 por errores de baja gravedad hasta $5000 por aquellos considerados como muy críticos, incentivando a los expertos en seguridad informática a contribuir a la mejora continua de la seguridad en la plataforma de Temu.

3. REFERENCIAS:

- https://cybersecuritynews.es/temu-se-suma-al-programa-de-recompensas-de-hackerone-para-fortalecer-su-ciberseguridad/

Ciberataque a camiones autónomos paraliza División Minera Gabriela Mistral de CODELCO

Tipo de Ataque: Diversos, Intrusión, Ciberataque

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- Camiones autónomos de Codelco y Komatsu
- Plataformas tecnológicas

2. RESUMEN:

La División Gabriela Mistral, ubicada en Sierra Gorda, Antofagasta, sufrió una interrupción de las operaciones de sus camiones autónomos por alrededor de 72 horas la semana pasada. Este suceso se atribuyó a un ciberataque, el incidente resalta la vulnerabilidad dentro de las tecnologías en la industria minera y la importancia de la ciberseguridad para asegurar la continuidad de las operaciones mineras.

3. DETALLE:

La División Gabriela Mistral constituye la segunda subdivisión de menor tamaño dentro de la corporación Codelco. Esta división opera la mina a tajo abierto ubicada en la comuna de Sierra Gorda, en la Región de Antofagasta, a una altitud de 2.660 metros sobre el nivel del mar. Una de sus destacadas características tecnológicas es que realiza sus actividades con el 100% de sus camiones de extracción de manera autónoma, prescindiendo de conductores, lo que la convierte en la primera empresa minera en el mundo en lograr trazabilidad del 100% en la producción de cátodos de cobre.

En la madrugada del miércoles 15 de noviembre 2023, los camiones autónomos del fabricante Komatsu comenzaron a fallar, reduciendo su operatividad notoriamente hasta el fin de semana.

La empresa explicó que “la plataforma tecnológica sobre la cual opera el servicio para la gestión del transporte autónomo de DGM presentó una disrupción mayor de seguridad”, atribuyendo esto a “una intervención maliciosa por parte de terceros no identificados”. Hasta el momento no se conoce con exactitud el tipo de ataque ni los autores de este.

La empresa desplego sus planes de contingencia para operar de forma manual una de las flotas y retomar las operaciones de forma parcial. Durante el viernes de la semana del incidente se configuro el reinicio del sistema, lo que permitió el retorno a la operación completa durante el fin de semana. Esto significo 72 horas de operación interrumpidas para DGM.

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.
- 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.statista.com/statistics/1224238/mining-metals-ceos-concern-about-company-cyber-attacks/
- https://www.timeline.cl/ciberataque-provoco-suspension-de-operaciones-de-camiones-autonomos-en-division-gabriela-mistral-de-codelco/#:~:text=Los%20camiones%20aut%C3%B3nomos%20de%20la,por%20alrededor%20de%2072%20horas
- https://www.latercera.com/pulso-pm/noticia/mas-problemas-en-codelco-el-ciberataque-que-golpeo-la-produccion-de-su-faena-gaby/DTTXYSMTCFAIXPXZYHECDZYYPU/

CISA está respondiendo a la explotación activa de PLCs Unitronics

Tipo de Ataque: Ciberataque

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- PLC de Unitronics

2. RESUMEN:

La Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) ha anunciado que está respondiendo a la explotación activa de controladores lógicos programables (PLCs) de Unitronics utilizados en sistemas de agua y aguas residuales (WWS) de WaterISAC. Los actores de amenazas cibernéticas probablemente accedieron al dispositivo afectado, un PLC de la serie Vision de Unitronics con una interfaz hombre-máquina (HMI), explotando debilidades de ciberseguridad, incluida una seguridad deficiente de contraseñas y exposición a Internet.

3. DETALLE:

CISA reveló que los actores de amenazas cibernéticas están dirigidos a PLCs asociados con instalaciones de WWS, incluido un PLC de Unitronics identificado, en una instalación de agua de EE. UU. En respuesta, la autoridad de agua afectada desconectó inmediatamente el sistema y pasó a operaciones manuales, asegurando que no hay riesgo conocido para el suministro de agua potable de la municipalidad.

La Policía Estatal de Pensilvania está investigando actualmente la explotación de Unitronics.

Las instalaciones del sector WWS utilizan PLCs para controlar y monitorear diversas etapas y procesos de tratamiento de agua y aguas residuales. CISA señala que los intentos de comprometer la integridad de WWS a través de acceso no autorizado amenazan la capacidad de estas instalaciones para proporcionar agua potable limpia y gestionar efectivamente las aguas residuales de sus comunidades.

Según informes locales, el grupo cibernético respaldado por Irán, CyberAv3ngers, atacó la Autoridad de Agua Municipal de Aliquippa en Pensilvania, tomando el control de una estación impulsora que regula la presión para los municipios de Raccoon y Potter. El dispositivo comprometido ha sido desactivado y se opera manualmente.

CISA insta a las organizaciones a cambiar la contraseña predeterminada del PLC de Unitronics y validar que **la contraseña predeterminada '1111'** no esté en uso. También recomienda la autenticación multifactor para el acceso remoto a la red OT, desconectar el PLC de Internet y, si es necesario el acceso remoto, implementar un firewall/VPN para controlar el acceso a la red remota. Unitronics ofrece un dispositivo de transporte a larga distancia seguro basado en celular.

Además, se insta a las organizaciones a realizar copias de seguridad de la lógica y configuraciones en los PLCs de Unitronics, actualizar a la última versión proporcionada por Unitronics y utilizar servicios de escaneo de vulnerabilidades cibernéticas. La WaterISAC seguirá monitoreando la situación y proporcionará información actualizada.

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:

- CISA responds to active exploitation of Unitronics PLCs in water and wastewater systems sector - Industrial Cyber
- https://www.ncsc.gov.uk/news/ncsc-statement-following-exploitation-of-unitronics-programmable-logic-controllers
- https://www.cybersecuritydive.com/news/cisa-threat-exploiting-unitronics-water/700999/