Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Octubre - 2025

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 Octubre.

Alertas de Seguridad IT:

- Askul Corp., empresa japonesa de comercio electrónico y suministros de oficina, sufre ataque de ransomware que paraliza sus operaciones
- Oracle, proveedor global de software empresarial, afectada por vulnerabilidad crítica explotada por el grupo de ransomware Cl0p
- Jewett-Cameron Company, fabricante estadounidense de productos para mascotas y cercas, sufre ataque de ransomware

Alertas de Seguridad OT/ICS:

- Heywood Healthcare, red hospitalaria estadounidense, sufre interrupción operativa tras ciberataque que afecta servicios clínicos y de comunicación
- Rosselkhoznadzor, organismo regulador alimentario ruso, sufre ataque DDoS que paraliza certificación de productos
- San Bernard Electric Cooperative y Karnes Electric Cooperative fueron víctimas de ataque de ransomware

Askul Corp., empresa japonesa de comercio electrónico y suministros de oficina, sufre ataque de ransomware que paraliza sus operaciones

Tipo de Ataque: Ransomware

Medio de Propagación: Red interna y sistemas de comercio electrónico comprometidos

1. **PRODUCTOS AFECTADOS:**
   - Plataformas de venta en línea Askul, Lohaco y Soloel Arena
   - Servicios de recepción y envío de pedidos
   - Canales de atención al cliente y solicitudes de devolución
   - Integraciones logísticas con socios comerciales como Ryohin Keikaku (Muji) y The Loft
2. **RESUMEN:**

El 20 de octubre, Askul Corp. confirmó un ataque de ransomware que ocasionó fallas críticas en sus sistemas, afectando el funcionamiento de sus tres portales de comercio electrónico. La compañía suspendió temporalmente la recepción de pedidos, los envíos y los servicios de atención al cliente. El incidente también impactó a Muji y The Loft, cuyos sitios web y operaciones logísticas se vieron interrumpidos al depender de los servicios de Askul. Actualmente, la empresa trabaja en la restauración de sus sistemas y evalúa si se produjo una filtración de datos de clientes.

3. **DETALLE:**

El ataque fue identificado como un ransomware que comprometió los sistemas internos de Askul, generando una interrupción total del entorno operativo. La infección afectó tanto los servidores de comercio electrónico como las integraciones con servicios logísticos y de facturación. Aunque no se ha confirmado la publicación de datos robados en portales de extorsión, el ataque provocó la suspensión inmediata de todas las transacciones electrónicas. Se presume que el vector inicial podría haber sido una vulnerabilidad en la red corporativa o un acceso no autorizado mediante credenciales comprometidas. La propagación del malware generó la cifrado de datos críticos, imposibilitando el acceso a sistemas de pedidos, catálogos y gestión de clientes. La dependencia de socios comerciales como Muji acentuó el impacto operativo en cadena. La compañía, subsidiaria de Yahoo! Japan Corporation, continúa el proceso de recuperación y ha iniciado investigaciones forenses para determinar la magnitud del daño y la posible exposición de información personal o empresarial.

4. **RECOMENDACIONES:**
   - Implementar copias de seguridad cifradas y desconectadas de la red principal.
   - Fortalecer los controles de acceso mediante autenticación multifactor (MFA).
   - Actualizar y parchear de inmediato todos los sistemas expuestos a Internet.
   - Realizar monitoreos continuos de tráfico de red para detectar comportamientos anómalos.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/retail-giant-muji-halts-online-sales-after-ransomware-attack-on-supplier/

Oracle, proveedor global de software empresarial, afectada por vulnerabilidad crítica explotada por el grupo de ransomware Cl0p

Tipo de Ataque: **Explotación de vulnerabilidad de día cero / Ransomware**

Medio de Propagación: **Acceso remoto a través de HTTP (Red externa / Internet)**

1. **PRODUCTOS AFECTADOS:**
   - Oracle E-Business Suite versiones 12.2.3 a 12.2.14
   - Componente Concurrent Processing (BI Publisher Integration)

2. **RESUMEN:**

El 26 de investigación. El grupo de ransomware Cl0p ha explotado una vulnerabilidad de día cero (CVE-2025-61882) en el producto Oracle E-Business Suite, calificada con un puntaje CVSS de 9.8. La falla permite la ejecución remota de código (RCE) sin autenticación a través del acceso HTTP. El ataque fue detectado a inicios de octubre de 2025, cuando varias organizaciones comenzaron a recibir demandas de rescate. Oracle lanzó un parche de seguridad el 4 de octubre de 2025 y emitió una alerta recomendando la actualización inmediata de sus sistemas.

3. **DETALLE:**

La vulnerabilidad se encuentra en el componente BI Publisher Integration del módulo Concurrent Processing de Oracle E-Business Suite. Un atacante remoto no autenticado puede aprovechar una cadena de cinco vulnerabilidades combinadas que permiten ejecutar código arbitrario antes de autenticarse en el sistema. Investigadores de Mandiant, Google Threat Intelligence Group y WatchTowr confirmaron que el exploit está activo en la red y disponible públicamente desde agosto de 2025. El grupo Cl0p, vinculado con Graceful Spider (asociado a Rusia), utiliza este vector para obtener acceso inicial y desplegar ransomware en entornos corporativos. Dado que la explotación se produce a través del acceso por HTTP, los sistemas de Oracle expuestos a Internet son altamente vulnerables. Las versiones afectadas incluyen aquellas que no han recibido las actualizaciones críticas de julio de 2025, lo que amplía el alcance del ataque. Oracle recomienda aplicar la Critical Patch Update de octubre de 2023 como requisito previo antes de instalar la corrección de la CVE-2025-61882, y verificar indicadores de compromiso (IoC) publicados en su aviso oficial.

4. **RECOMENDACIONES:**
   - Actualizar inmediatamente a la versión más reciente de Oracle E-Business Suite y aplicar el parche oficial de Oracle.
   - Restringir el acceso remoto HTTP a los módulos de Oracle E-Business Suite no esenciales.
   - Implementar monitoreo continuo de actividad sospechosa en los servidores de aplicaciones Oracle.
   - Fortalecer políticas de respaldo y recuperación ante ransomware, asegurando copias desconectadas de la red.

5. **REFERENCIAS:**
   - https://www.securityweek.com/oracle-e-business-suite-zero-day-exploited-in-cl0p-attacks/

Jewett-Cameron Company, fabricante estadounidense de productos para mascotas y cercas, sufre ataque de ransomware

Tipo de Ataque: **Ransomware / Doble extorsión / Robo de información**

Medio de Propagación: **Intrusión en red corporativa a través de sistemas IT internos**

1. **PRODUCTOS AFECTADOS:**
   - Sistemas corporativos de Jewett-Cameron Company
   - Aplicaciones de negocio relacionadas con operaciones y funciones financieras
   - Servidores que almacenan datos de video reuniones e información administrativa

2. **RESUMEN:**

El 15 de octubre, Jewett-Cameron Company, fabricante de productos para mascotas, cercas y jardinería con sede en Oregón, detectó una intrusión en su entorno IT que resultó en la instalación de software de cifrado y monitoreo. El ataque interrumpió parcialmente las operaciones corporativas e impidió el acceso a ciertas aplicaciones críticas. La investigación determinó que los atacantes exfiltraron información confidencial, incluyendo imágenes de videollamadas y pantallas corporativas con datos financieros. Los delincuentes amenazan con publicar la información robada si no se paga un rescate. La empresa confirmó que se trata de un ataque de doble extorsión con cifrado y robo de datos.

3. **DETALLE**

El ataque consistió en la comprometida de los sistemas IT corporativos, donde los atacantes desplegaron herramientas de ransomware con capacidades de cifrado y espionaje. Estas incluyeron software para registrar actividad en pantalla y capturar imágenes de reuniones virtuales, así como utilidades para cifrar archivos críticos. La evidencia sugiere que los actores obtuvieron acceso mediante credenciales comprometidas o vulnerabilidades en servicios expuestos, lo que permitió la instalación de software de monitoreo persistente antes de ejecutar la fase de cifrado. Los datos sustraídos incluyen principalmente información interna y financiera vinculada a los reportes anuales ante la SEC (Securities and Exchange Commission). Aunque no se ha confirmado el grupo atacante, el modus operandi coincide con tácticas de ransomware de doble extorsión, en las que los agresores combinan cifrado de datos y amenazas de publicación. La empresa ha contenido el incidente y está restaurando los sistemas, apoyada por su póliza de ciberseguro.

4. **RECOMENDACIONES:**
   - Implementar revisiones exhaustivas de acceso remoto y autenticación multifactor para todos los sistemas críticos.
   - Realizar copias de seguridad cifradas y almacenarlas fuera de la red principal (offline).
   - Fortalecer la segmentación de red y desarrollar un plan de respuesta ante ransomware que incluya manejo de comunicación, extorsión y recuperación.

5. **REFERENCIAS:**
   - https://www.securityweek.com/fencing-and-pet-company-jewett-cameron-hit-by-ransomware/

Heywood Healthcare, red hospitalaria estadounidense, sufre interrupción operativa tras ciberataque que afecta servicios clínicos y de comunicación

Tipo de Ataque: Interrupción de servicios / Compromiso de red

Medio de Propagación: Red interna e infraestructura de comunicaciones corporativas

1. PRODUCTOS AFECTADOS:

- Sistemas de red interna y de comunicación de Heywood Healthcare
- Servicios clínicos digitales: radiología, laboratorio y urgencias
- Portales de atención y gestión hospitalaria

2. RESUMEN:

Los hospitales Heywood y Athol, pertenecientes a Heywood Healthcare, experimentaron una interrupción significativa de red tras un ciberataque detectado la semana pasada. El incidente provocó el cierre temporal del servicio de urgencias y la desviación de ambulancias a otros centros debido a la falta de acceso a sistemas críticos. También se interrumpieron los servicios de radiología, laboratorio y correo electrónico. Aunque parte de las comunicaciones se han restablecido, la funcionalidad completa aún no se ha recuperado. La organización trabaja junto a una firma externa de ciberseguridad y las autoridades competentes para investigar el origen del ataque y determinar si hubo filtración de datos de pacientes.

3. DETALLE:

El ataque comprometió la infraestructura IT hospitalaria, afectando conectividad a Internet, servidores de correo y telefonía, así como los sistemas clínicos en red. La organización activó su protocolo de respuesta a incidentes (Código Negro) y aisló los sistemas afectados para contener la propagación. Aunque no se ha confirmado oficialmente, las características del incidente sugieren un posible ataque de ransomware o intrusión con interrupción deliberada de servicios. La desconexión preventiva impidió la continuidad de servicios críticos y generó un impacto directo en la atención médica. Heywood Healthcare señaló que, hasta el momento, no existen indicios confirmados de robo de información sensible, pero la investigación continúa.

4. RECOMENDACIONES:

- Segregar redes hospitalarias críticas (equipos médicos, laboratorios, registros) de redes administrativas y de usuario.
- Actualizar y reforzar las configuraciones de seguridad en servidores de correo, telefonía IP y portales hospitalarios.
- Auditar los accesos a sistemas clínicos y reforzar autenticación multifactor para personal médico y técnico.

5. REFERENCIAS:

- https://www.hipaajournal.com/heywood-athol-hospitals-cyberattack/

Rosselkhoznadzor, organismo regulador alimentario ruso, sufre ataque DDoS que paraliza certificación de productos

Tipo de Ataque: Ataque de Denegación de Servicio Distribuido (DDoS)

Medio de Propagación: Tráfico masivo malicioso dirigido a la plataforma Mercury

1. **PRODUCTOS AFECTADOS:**
   - Plataforma Mercury (sistema de certificación veterinaria)
   - Servicios de validación para envíos de carne, leche y alimentos infantiles
2. **RESUMEN:**

El 22 de octubre de 2025, Rosselkhoznadzor, la agencia rusa encargada de la certificación alimentaria, sufrió un ataque DDoS que dejó inoperativa la plataforma Mercury durante varias horas. Esto impidió la emisión de certificados veterinarios, bloqueando la distribución de productos perecederos y generando pérdidas significativas, pese a declaraciones oficiales que minimizaron el impacto.

3. **DETALLE:**

El ataque comenzó a las 08:40 (hora de Moscú) y saturó los sistemas de Rosselkhoznadzor con tráfico malicioso, afectando la disponibilidad del servicio. Aunque la agencia afirmó que no hubo compromiso de datos, empresas reportaron imposibilidad de emitir certificados, lo que detuvo envíos y obligó a desechar productos perecederos. El ataque se mitigó con la colaboración de operadores como Megafon, Rostelecom e Intellex, quienes filtraron el tráfico. No se identificaron intentos de intrusión en bases de datos ni explotación de vulnerabilidades, pero el incidente evidencia la fragilidad de sistemas críticos ante ataques volumétricos. Además, la falta de transparencia en la comunicación oficial generó incertidumbre en el sector alimentario, amplificando el impacto económico. Este evento refuerza la necesidad de planes de contingencia y soluciones anti-DDoS robustas para garantizar la continuidad operativa en infraestructuras críticas.

4. **RECOMENDACIONES:**
   - Implementar soluciones anti-DDoS en la infraestructura crítica.
   - Configurar redundancia y balanceo de carga para servicios esenciales.
   - Restringir exposición directa de plataformas críticas en internet.
   - Activar monitoreo en tiempo real y alertas para anomalías de tráfico.
   - Establecer planes de contingencia para garantizar continuidad operativa.
   - Coordinar con proveedores de telecomunicaciones para filtrado proactivo.
5. **REFERENCIAS:**

- https://www.bitdefender.com/en-us/blog/hotforsecurity/hackers-russia-food-hackers-ukraine-war

San Bernard Electric Cooperative y Karnes Electric Cooperative fueron víctimas de ataque de ransomware

Tipo de Ataque: Ransonware

Medio de Propagación: Acceso remoto a sistemas corporativos y filtración en sitio de leaks en la dark web

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de gestión financiera y operativa
   - Documentos internos (contratos, reportes, credenciales)
   - Plataformas administrativas vinculadas a la red eléctrica
2. **RESUMEN:**

El grupo de ransomware Qilin, vinculado a Rusia, afirmó haber comprometido dos cooperativas eléctricas en Texas: San Bernard Electric Cooperative y Karnes Electric Cooperative. Los atacantes publicaron muestras de datos financieros y personales en su sitio de filtraciones, incluyendo contratos, reportes de gastos y listas de directores. El incidente afecta infraestructura crítica y podría impactar la continuidad operativa y la reputación de las organizaciones.

3. **DETALLE:**

El grupo Qilin afirmó haber comprometido los sistemas internos de San Bernard Electric Cooperative y Karnes Electric Cooperative, dos entidades que gestionan más de 8,900 millas de líneas eléctricas y abastecen a más de 51,000 hogares en Texas. El ataque sigue el patrón de doble extorsión, donde los atacantes cifran sistemas y publican muestras de datos en su sitio de filtraciones en la dark web para presionar el pago del rescate. Las muestras analizadas incluyen información altamente sensible: reportes de incidentes con datos personales (nombres, teléfonos), presupuestos anuales, contratos de servidumbre, documentos de seguros, facturas, listas de directores con direcciones y balances financieros diarios. Esta exposición representa riesgos críticos como robo de identidad e ingeniería social dirigida a altos ejecutivos. Aunque no se ha confirmado la autenticidad completa de los datos, Qilin ha demostrado capacidad operativa en ataques previos contra sectores críticos (salud, manufactura, telecomunicaciones). El incidente subraya la vulnerabilidad de la infraestructura energética ante ataques que, aunque inicialmente afectan entornos IT, pueden facilitar movimientos laterales hacia sistemas OT (SCADA, HMI) si no existe segmentación adecuada.

4. **RECOMENDACIONES:**
   - Aislar sistemas comprometidos y ejecutar análisis forense.
   - Implementar segmentación estricta entre redes IT y OT.
   - Activar monitoreo continuo en SIEM para detectar movimientos laterales.
   - Aplicar parches y reforzar autenticación multifactor en accesos remotos.
   - Capacitar al personal en prevención de ingeniería social y phishing.

5. **REFERENCIAS:**

- https://cybernews.com/security/texas-electric-coops-ransomware-attack/