Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Enero - 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 septiembre.

Alertas de Seguridad IT:

- DeepSeek expone bases de datos con registros de usuarios y credenciales sensibles
- Ciberdelincuentes despliegan ransomware a través de llamadas en Microsoft Teams
- Hacker IntelBroker vende información robada de HPE, incluyendo código fuente y credenciales

Alertas de Seguridad OT/ICS:

- Rockwell Automation corrige vulnerabilidades críticas y de alta severidad en múltiples productos
- Investigadores descubren más de 1,000 vulnerabilidades en sistemas de automatización de edificios de ABB

DeepSeek expone bases de datos con registros de usuarios y credenciales sensibles

Tipo de Ataque: **Exposición de datos sensibles.**

Medio de Propagación: **Bases de dato**

1. **PRODUCTOS AFECTADOS:**
   - Registros internos de DeepSeek, incluyendo historial de chat en texto plano, claves API y metadatos operativos.
   - Infraestructura interna y servicios de autenticación expuestos.

2. **RESUMEN:**

Wiz Research descubrió que DeepSeek, la startup china de IA conocida por su modelo DeepSeek-R1, expuso dos bases de datos sin medidas de seguridad adecuadas. Estas contenían más de un millón de registros, incluyendo el historial de chat de usuarios en texto plano, credenciales de autenticación de backend y detalles de infraestructura interna.

Los servidores en oauth2callback.deepseek.com:9000 y dev.deepseek.com:9000 permitían ejecutar consultas SQL arbitrarias sin autenticación, lo que representaba un riesgo crítico tanto para DeepSeek como para sus usuarios. Wiz alertó a la empresa, que rápidamente cerró el acceso público a las bases de datos

3. **DETALLE:**

Las bases de datos expuestas contenían una tabla llamada log_stream con registros sensibles desde el 6 de enero de 2025, incluyendo:

- Consultas de usuarios al chatbot de DeepSeek.
- Claves API utilizadas por sistemas internos.
- Información sobre infraestructura y servicios internos.
- Metadatos operativos críticos.

Además, la falta de restricciones adecuadas podría haber permitido a atacantes ejecutar consultas más intrusivas, como la exfiltración de archivos locales o credenciales en texto plano mediante comandos SQL avanzados (SELECT * FROM file('filename')). No se ha confirmado si actores maliciosos accedieron a estos datos antes de la intervención de Wiz.

Este incidente se suma a recientes problemas de seguridad en DeepSeek, que incluyen ciberataques persistentes que obligaron a la empresa a suspender nuevos registros de usuarios durante 24 horas.

4. **RECOMENDACIONES:**
   - Configurar adecuadamente las bases de datos expuestas a Internet, asegurando autenticación y restricciones de acceso.
   - Implementar monitoreo continuo para detectar accesos no autorizados y exposiciones accidentales de datos.

- Revisar y rotar credenciales comprometidas para evitar accesos indebidos a infraestructura crítica.
- Aplicar cifrado a datos sensibles almacenados para mitigar el riesgo de exposición en caso de brechas.
- Realizar auditorías de seguridad periódicas para identificar y corregir configuraciones erróneas en entornos de producción.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/deepseek-exposes-database-with-over-1-million-chat-records/

Ciberdelincuentes despliegan ransomware a través de llamadas en Microsoft Teams

Tipo de Ataque: Ingeniería social

Medio de Propagación: Ataques de phishing y uso de herramientas

1. **PRODUCTOS AFECTADOS:**
   - Microsoft Teams
2. **RESUMEN:**

Investigadores de Sophos Managed Detection and Response (MDR) han identificado dos campañas de ransomware, STAC5143 y STAC5777, que explotan Microsoft Teams para infiltrarse en organizaciones. Los atacantes aprovechan configuraciones por defecto que permiten interacciones con usuarios externos y utilizan ingeniería social para engañar a las víctimas.

El ataque se lleva a cabo en múltiples fases:

- Email Bombing: Envío masivo de hasta 3,000 correos electrónicos en una hora para saturar y distraer a los usuarios.
- Ingeniería Social: Suplantación de IT support para engañar a las víctimas mediante llamadas en Teams.
- Acceso Remoto: Uso de Microsoft Quick Assist o la función de control remoto en Teams para tomar el control del sistema.
- Despliegue de Malware: Ejecución de payloads maliciosos para comprometer el sistema y desplegar ransomware.

3. **DETALLE**

Campaña STAC5143

Esta campaña utiliza archivos Java Archive (JAR) y puertas traseras en Python para mantener acceso persistente en los sistemas comprometidos. Una de sus tácticas clave es la implementación de RPivot, un proxy SOCKS inverso ofuscado que permite el tráfico encubierto y la persistencia en la red de la víctima.

Para evadir detección, los atacantes usan funciones lambda para la ofuscación de código, una técnica similar a la utilizada por FIN7. Además, establecen comunicación con servidores C2 a través del puerto 80, imitando tráfico HTTP legítimo para evitar ser detectados.

Campaña STAC5777

En esta campaña, los atacantes utilizan una DLL maliciosa llamada winhttp.dll, que es cargada lateralmente por el ejecutable legítimo OneDriveStandaloneUpdater.exe. También emplean controladores OpenSSL no firmados para establecer comunicación con servidores C2, lo que les permite controlar los dispositivos infectados sin levantar sospechas.

Para mantener el acceso persistente, modifican el registro de Windows en HKLM\SOFTWARE\TitanPlus y crean servicios y accesos directos (.lnk) para asegurarse de que el malware se ejecute tras un reinicio.

Además, realizan escaneos SMB para moverse lateralmente en la red y tratan de desinstalar software de seguridad y soluciones MFA, debilitando aún más la protección de los sistemas comprometidos.

Uno de los intentos detectados por Sophos mostró que STAC5777 intentó desplegar el ransomware Black Basta, aunque la amenaza fue bloqueada por las soluciones de protección de endpoints de Sophos.

El malware utilizado en estas campañas tiene capacidades avanzadas, entre ellas:

- Recolección de detalles del sistema y el sistema operativo.
- Captura de credenciales de usuario.
- Registro de pulsaciones de teclas mediante funciones de la API de Windows.
- Exploración de redes y movimiento lateral.
- Exfiltración de datos sensibles.

4. RECOMENDACIONES:

- Educar a los empleados sobre ataques de ingeniería social, especialmente aquellos que aprovechan plataformas de comunicación como Teams.
- Restringir las llamadas de Microsoft Teams desde entidades externas para reducir el riesgo de ataques de ingeniería social.
- Limitar el uso de herramientas de acceso remoto, como Microsoft Quick Assist, e implementar controles de aplicaciones para evitar su ejecución no autorizada.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/microsoft-teams-phishing-attack-alerts-coming-to-everyone-next-month/

Hacker IntelBroker vende información robada de HPE, incluyendo código fuente y credenciales

Tipo de Ataque: Fuga de datos

Medio de Propagación: Explotación de vulnerabilidades en los sistemas

1. **PRODUCTOS AFECTADOS:**
   - Servicios internos de HPE, como APIs, WePay, GitHub y GitLab.
2. **RESUMEN:**

El hacker IntelBroker anunció en un foro de cibercrimen el 16 de enero la venta de información robada de HPE. Los datos comprometidos incluyen código fuente de productos críticos, repositorios privados, credenciales, certificados digitales y acceso a servicios internos de la compañía. HPE ha confirmado que está al tanto de las afirmaciones y ha iniciado una investigación para evaluar la validez del incidente. Hasta el momento, la empresa afirma que no hay impacto operativo ni evidencia de que información de clientes haya sido expuesta.

IntelBroker ha estado detrás de múltiples ataques a grandes empresas en los últimos años, incluyendo Cisco, que en su momento confirmó la autenticidad de datos filtrados, aunque minimizó su impacto.

3. **DETALLE**

El atacante afirma haber accedido a datos sensibles dentro de los sistemas de HPE, incluyendo información interna de desarrollo y credenciales de acceso. Entre los productos comprometidos se encuentran soluciones clave como Zerto e iLO, cuya filtración podría permitir a actores maliciosos desarrollar exploits o manipular infraestructura crítica.

IntelBroker también asegura tener acceso a servicios internos utilizados por HPE, lo que podría permitir ataques posteriores o movimientos laterales dentro de la infraestructura de la empresa. La compañía ha tomado medidas inmediatas, como la desactivación de credenciales comprometidas y la implementación de protocolos de respuesta ante incidentes.

4. **RECOMENDACIONES:**
   - Rotar y reforzar credenciales: Implementar autenticación multifactor y evitar el uso de contraseñas repetidas o débiles.
   - Monitoreo de accesos y actividad sospechosa: Revisar logs de acceso a repositorios y sistemas internos para detectar posibles intrusiones.
   - Protección de código fuente y certificados: Implementar cifrado fuerte y medidas de control de acceso en repositorios de desarrollo.
5. **REFERENCIAS:**
   - https://www.securityweek.com/hpe-investigating-breach-claims-after-hacker-offers-to-sell-data/

Rockwell Automation corrige vulnerabilidades críticas y de alta severidad en múltiples productos

Tipo de Ataque: Ejecución remota de comandos, ejecución de código local, exposición de credenciales y denegación de servicio (DoS)

Medio de Propagación: Explotación de vulnerabilidades en software

1. **PRODUCTOS AFECTADOS:**
   - FactoryTalk View Machine Edition.
   - FactoryTalk View Site Edition
   - DataMosaix Private Cloud
   - ICE2 Controller
   - PowerFlex 755
   - KEPServer
2. **RESUMEN:**

Rockwell Automation ha lanzado parches para corregir vulnerabilidades críticas y de alta severidad en sus productos de automatización industrial. Entre ellas, destacan fallas de ejecución remota de comandos, acceso no autenticado a configuraciones y exposición de credenciales.

CISA ha emitido alertas sobre estos problemas, y aunque no se ha detectado explotación activa, se recomienda su mitigación inmediata para evitar riesgos en infraestructuras críticas.

3. **DETALLE:**

En la plataforma DataMosaix Private Cloud, Rockwell corrigió una vulnerabilidad crítica relacionada con SQLite, originalmente parcheada en 2020, y una falla de path traversal que expone información sensible.Adicionalmente, se solucionaron una vulnerabilidad de denegación de servicio (DoS) en el ICE2 Controller y una falla de exposición de credenciales en PowerFlex 755.

El KEPServer también recibió un parche tras la identificación de una vulnerabilidad DoS explotada por investigadores de Claroty durante la competencia Pwn2Own 2023.

Las vulnerabilidades en los productos de Rockwell Automation afectan tanto a software como hardware de automatización industrial. Entre los principales riesgos se encuentran:

- Ejecución remota de comandos en FactoryTalk View Machine Edition, lo que permitiría a un atacante tomar control del sistema afectado.
- Acceso no autorizado a configuraciones del sistema en FactoryTalk View Site Edition, lo que expone la infraestructura a posibles manipulaciones.
- Exposición de credenciales en PowerFlex 755, que podría facilitar movimientos laterales dentro de la red.
- Denegación de servicio (DoS) en ICE2 Controller y KEPServer, lo que podría generar interrupciones operativas en entornos industriales.

4. **RECOMENDACIONES:**
   - Aplicar los parches de seguridad proporcionados por Rockwell Automation de manera inmediata para mitigar los riesgos asociados.

- Monitorear el tráfico y actividad en los sistemas afectados para detectar intentos de explotación de estas vulnerabilidades.
- Revisar y reforzar credenciales de acceso en los productos comprometidos para evitar la exposición de información sensible.
- Implementar segmentación de red y controles de acceso para minimizar el impacto en caso de explotación de alguna de estas fallas.
- Actualizar y auditar periódicamente los sistemas de automatización industrial, priorizando vulnerabilidades conocidas en componentes críticos.

5. REFERENCIAS:

- https://www.securityweek.com/rockwell-patches-critical-high-severity-vulnerabilities-in-several-products/

Investigadores descubren más de 1,000 vulnerabilidades en sistemas de automatización de edificios de ABB

Tipo de Ataque: Vulnerabilidades

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- ABB Cylon FLXeon
- ABB Cylon Aspect

2. RESUMEN:

El investigador Gjoko Krstic identificó más de 1,000 vulnerabilidades en los sistemas ABB Cylon Aspect (incluyendo fallos de severidad crítica y alta) y 35 fallos en el producto FLXeon. Estas vulnerabilidades permiten a atacantes remotos no autenticados ejecutar código, acceder a información sensible, manipular archivos o causar interrupciones en sistemas de automatización de edificios. ABB ha publicado parches, pero se estima que alrededor de 1,000 instalaciones en todo el mundo exponen estos sistemas a Internet, lo que los hace vulnerables a ataques que podrían alterar sistemas de iluminación, HVAC, presión de agua, puertas y controles industriales (ICS).

3. DETALLE:

El investigador Gjoko Krstic identificó 1,035 vulnerabilidades en los sistemas de automatización de edificios ABB Cylon Aspect (1,000 fallos) y ABB Cylon FLXeon (35 fallos). Entre las vulnerabilidades más críticas destacan:

- Ejecución remota de código (RCE) a través de fallos en la gestión de contraseñas o inyecciones SQL.
- Exposición de datos sensibles por SSRF (Server-Side Request Forgery), permitiendo acceder a redes internas.
- Manipulación no autorizada de sistemas HVAC, presión de agua, puertas y sensores mediante IDOR (Insecure Direct Object Reference).
- Denegación de servicio (DoS) que podría paralizar operaciones en instalaciones críticas.

Krstic señaló que al menos 15% de las vulnerabilidades en el sistema Aspect fueron clasificadas como críticas (CVSS ≥ 9.0), incluyendo casos donde un atacante remoto y no autenticado podría tomar control total del dispositivo. Por ejemplo, una sola solicitud HTTP maliciosa podría alterar la configuración de alarmas de incendio o iluminación en hospitales.

ABB ha lanzado parches, pero el investigador advierte que aproximadamente 1,000 instalaciones en todo el mundo aún exponen estos sistemas a Internet, ignorando las recomendaciones de seguridad. Esto incluye hospitales, aeropuertos y estadios donde un ataque podría causar:

- Interrupciones en quirófanos por manipulación de presión de agua.

- Caos en eventos masivos al bloquear puertas o alterar ventilación.
- Corrupción de datos en sistemas industriales mediante inyecciones SQL.

Aunque ABB ha corregido los fallos, la actualización de sistemas BMS (Building Management Systems) en infraestructuras críticas (que operan 24/7) suele retrasarse, ampliando las ventanas de exposición.

4. RECOMENDACIONES:

- Aplicar inmediatamente los parches proporcionados por ABB para los sistemas Cylon FLXeon y Aspect.
- Restringir el acceso a Internet de los sistemas de automatización de edificios y utilizar segmentación de redes para aislarlos.
- Implementar controles de acceso estrictos (MFA, autenticación robusta) y monitorear tráfico sospechoso en redes OT/IoT.

5. REFERENCIAS:

- https://www.securityweek.com/researcher-says-abb-building-control-products-affected-by-1000-vulnerabilities/