Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

31-Ene-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 Enero.

Alertas de Seguridad IT:

- ChatGPT puede ser usado para hackear páginas Web.
- Dos vulnerabilidades críticas en Enrutadores Cisco Small Business sin remediación.
- Zoom parcha vulnerabilidades de alto riesgo en Windows y MacOS.

Alertas de Seguridad OT/ICS:

- Vulnerabilidad Crítica en SINEC INS de Siemens.
- Vulnerabilidad Alta en la solución de mantenimiento predictivo de equipos RONDS.

ChatGPT puede ser usado para hackear páginas Web

Tipo de Ataque: **Abuso de inteligencia artificial**

Medio de Propagación: **Sistemas web en general**

1. **PRODUCTOS AFECTADOS:**

- Sistemas web en general

2. **RESUMEN:**

La habilidad y detalladas bases de conocimiento del recientemente lanzado chat GPT pueden ser usadas para asistir paso a paso a un atacante, aun cuando éste no tenga muchos conocimientos.

3. **DETALLE:**

ChatGPT es un sistema de chat basado en el modelo de lenguaje por Inteligencia Artificial desarrollado por OpenAI. Esta inteligencia artificial es entrenada a base de texto y permite brindar respuestas cada vez más precisas a los usuarios.

Investigadores de Cybernews han puesto a prueba ChatGPT para guiarlos en supuesto reto académico, pero que en realidad era una plataforma de "Hack the Box" que sirve para entrenar ethical hackers. Sin embargo, el mismo mecanismo podría usarse para hackear el sitio web operativo de una organización real. El chat conversacional da instrucciones de como detectar y utilizar las vulnerabilidades. Su capacidad de contextualizar las preguntas permite ir avanzando en la intrusión y seguir preguntando mayores detalles. También se ha reportado que ChatGPT puede ayudar a escribir código malicioso.

Si bien ChatGPT ha sido diseñado para rechazar preguntas inapropiadas y responde enfatizando que hackear es ilegal, no deja por ello de responder consultas técnicas que se le pregunten. Por lo que puede ser utilizada como herramienta para facilitar las tareas de hacking.

4. **RECOMENDACIONES:**

- Con tantas herramientas al alcance de los diferentes actores de riesgo, se debe continuar con las buenas prácticas de hardening, detección y gestión de vulnerabilidades.

5. **REFERENCIAS:**

- https://cybernews.com/security/hackers-exploit-chatgpt/

Dos vulnerabilidades críticas en Enrutadores Cisco Small Business sin remediación

Tipo de Ataque: Bypass de autenticación

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- RV016 Multi-WAN VPN Routers
- RV042 Dual WAN VPN Routers
- RV042G Dual Gigabit WAN VPN Routers
- RV082 Dual WAN VPN Routers

2. RESUMEN:

Cisco ha reportado dos vulnerabilidades de severidad CRÍTICA de tipo **omisión de autenticación** y **ejecución remota de comandos** en la interfaz de administración basada en la web de los enrutadores Cisco Small Business RV016, RV042, RV042G y RV082. Al cierre de esta nota, Cisco no ha publicado actualizaciones de software para abordar las vulnerabilidades descritas en este aviso. No hay soluciones alternativas que aborden estas vulnerabilidades.

3. DETALLE:

Una vulnerabilidad en la interfaz de administración basada en la web de los enrutadores Cisco Small Business RV016, RV042, RV042G y RV082 podría permitir que un atacante remoto no autenticado omita el proceso de autenticación en un dispositivo afectado.

Esta vulnerabilidad se debe a una validación incorrecta de la entrada del usuario dentro de los paquetes HTTP entrantes. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP manipulada a la interfaz de administración basada en web. Una explotación exitosa podría permitir al atacante eludir la autenticación y obtener acceso de root en el sistema operativo subyacente.

Cisco anunció que "*no ha publicado ni publicará*" actualizaciones de software que aborden esta vulnerabilidad, dado que se descontinuó el soporte a estos hardware el 2021. No hay soluciones alternativas que aborden esta vulnerabilidad.

A continuación, la lista de productos confirmados como NO Vulnerables:

- RV160 VPN Routers
- RV160W Wireless-AC VPN Routers
- RV260 VPN Routers
- RV260P VPN Routers with PoE
- RV260W Wireless-AC VPN Routers
- RV320 Dual Gigabit WAN VPN Routers
- RV325 Dual Gigabit WAN VPN Routers
- RV340 Dual WAN Gigabit VPN Routers
- RV340W Dual WAN Gigabit Wireless-AC VPN Routers
- RV345 Dual WAN Gigabit VPN Routers

- RV345P Dual WAN Gigabit PoE VPN Routers

4. RECOMENDACIONES:

- No hay soluciones alternativas que aborden estas vulnerabilidades. Sin embargo, los administradores pueden mitigar las vulnerabilidades al deshabilitar la administración remota y bloquear el acceso a los puertos 443 y 60443. Los enrutadores seguirán siendo accesibles a través de la interfaz LAN después de que se haya implementado la mitigación.

5. REFERENCIAS:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-productos-cisco-85
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20025

Zoom parcha vulnerabilidades de alto riesgo en Windows y MacOS

Tipo de Ataque: **Elevación de privilegios**

Medio de Propagación: **Red, Internet**

1. PRODUCTOS AFECTADOS:

- Zoom Rooms for Windows installers before version 5.13.0
- Zoom Rooms for Windows clients before version 5.12.7
- Zoom Rooms for macOS clients before version 5.11.3

2. RESUMEN:

El gigante de la mensajería de video, Zoom, ha lanzado parches para múltiples vulnerabilidades de seguridad que exponen a los usuarios de Windows y macOS a ciberataques. Las vulnerabilidades, en el producto Zoom Rooms para empresas, podrían explotarse en ataques de escalamiento de privilegios en plataformas Windows y macOS.

3. DETALLE:

El lote de parches incluye parches para 3 vulnerabilidades de severidad alta:

- CVE-2022-36930: escalamiento de privilegios locales en Zoom Rooms para instaladores de Windows (CVSS 8.2/10). Los instaladores de Zoom Rooms para Windows anteriores a la versión 5.13.0 contienen una vulnerabilidad de escalamiento de privilegios locales. Un usuario local con pocos privilegios podría explotar esta vulnerabilidad en una cadena de ataque para escalar sus privilegios al usuario del SISTEMA.
- CVE-2022-36929: escalamiento de privilegios locales en Zoom Rooms para clientes de Windows (CVSS 7.8/10). Los clientes de Zoom Rooms para Windows anteriores a la versión 5.12.7 contienen una vulnerabilidad de escalamiento de privilegios locales. Un usuario local con pocos privilegios podría explotar esta vulnerabilidad en una cadena de ataque para escalar sus privilegios al usuario del SISTEMA.
- CVE-2022-36927: escalamiento de privilegios locales en Zoom Rooms para clientes macOS (CVSS 8.8/10). Zoom Rooms para clientes macOS anteriores a la versión 5.11.3 contiene una vulnerabilidad de aumento de privilegios local. Un usuario local con pocos privilegios podría aprovechar esta vulnerabilidad para escalar sus privilegios a root.

Zoom también lanzó correcciones para un par de errores de gravedad media en Zoom Rooms para clientes macOS antes de la versión 5.11.4, advirtiendo que esta versión del software contiene un mecanismo de generación de claves inseguro.

4. RECOMENDACIONES:

- Aplicar el lote de parches para los productos afectados.

5. REFERENCIAS:

- https://nvd.nist.gov/vuln/detail/CVE-2022-36930

- https://nvd.nist.gov/vuln/detail/CVE-2022-36929
- https://nvd.nist.gov/vuln/detail/CVE-2022-36927

Vulnerabilidad Crítica en SINEC INS de Siemens

Tipo de Ataque: Inyección de comandos OS, Insuficiente nivel de encriptación y varios más

Medio de Propagación: Red, Internet

1. PRODUCTOS AFECTADOS:

- SINEC INS: versiones anteriores a V1.0 SP2 Update 1.

*SINEC INS es la herramienta de software de Siemens para los servicios de red central, que se utiliza en el campo de la Tecnología Operacional (OT)

2. RESUMEN:

Se detectaron diversas vulnerabilidades explotables remotamente y de baja complejidad para su ejecución. La explotación exitosa de estas podría permitir que un atacante lea y escriba archivos arbitrarios del sistema de archivos del componente afectado y, en última instancia, ejecute código arbitrario en el dispositivo.

3. DETALLE:

Las vulnerabilidades reportadas son:

Codificación CVE	CVSS v3	Descripción
CVE-2022-45092	9.9	PATH TRAVERSAL CWE-22
CVE-2022-2068	9.8	OS COMMAND INJECTION CWE-78
CVE-2022-2274	9.8	OUT-OF-BOUNDS WRITE CWE-787
CVE-2022-35256	9.8	AUTHENTICATION BYPASS BY SPOOFING CWE-290
CVE-2022-45093	8.5	PATH TRAVERSAL CWE-22
CVE-2022-45094	8.4	COMMAND INJECTION CWE-77
CVE-2022-32212	8.1	OS COMMAND INJECTION CWE-78
CVE-2022-35255	7.5	USE OF INSUFFICIENTLY RANDOM VALUES CWE-330
CVE-2022-32213	6.5	HTTP REQUEST SMUGGLING CWE-444
CVE-2022-32215	6.5	HTTP REQUEST SMUGGLING CWE-444
CVE-2022-2097	5.3	INADEQUATE ENCRYPTION STRENGTH CWE-326
CVE-2022-32222	5.3	INADEQUATE ENCRYPTION STRENGTH CWE-326

Tabla 1: Lista de vulnerabilidades reportadas

4. RECOMENDACIONES:

Recomendamos actualizar a la última versión publicada.

Siemens identificó las siguientes soluciones y mitigaciones específicas que los usuarios pueden aplicar para reducir el riesgo:

- CVE-2022-45094: deshabilite el servicio DHCP del producto afectado, si no es necesario.

- CVE-2022-45093: deshabilite el servicio SFTP del producto afectado, si no es necesario.

Como medida de seguridad general, recomendamos proteger el acceso a la red a los dispositivos con los mecanismos adecuados. Para operar los dispositivos en un entorno de IT protegido, Siemens recomienda configurar el entorno de acuerdo con "Operational Guidelines for Industrial Security" de Siemens y seguir las recomendaciones de los manuales del producto. Siemens ha publicado también "Additional information on industrial security".

Como recomendaciones generales para un entorno OT:

- Asegúrese de que se siga el principio de mínimo privilegio.
- Minimice la exposición de la red para todos los dispositivos y/o sistemas del sistema de control, y asegúrese de que no sean accesibles desde Internet.
- Ubique las redes de sistemas de control y dispositivos remotos detrás de firewalls y aíslelos de las redes comerciales.
- Cuando se requiera acceso remoto, use métodos seguros, como Redes Privadas Virtuales (VPN), reconociendo que las VPN pueden tener vulnerabilidades y deben actualizarse a la versión más reciente disponible. También reconozca que VPN es tan segura como sus dispositivos conectados.

Adicionalmente, se recomienda a las organizaciones realizar un análisis de impacto y una evaluación de riesgos adecuados antes de implementar medidas defensivas.

5. REFERENCIAS:

- https://www.cisa.gov/uscert/ics/advisories/icsa-23-017-03
- https://nvd.nist.gov/vuln/detail/CVE-2022-45094
- https://nvd.nist.gov/vuln/detail/CVE-2022-45093
- https://nvd.nist.gov/vuln/detail/CVE-2022-45092

Vulnerabilidad Alta en la solución de mantenimiento predictivo de equipos RONDS

Tipo de Ataque: Exposición de información sensible / Insuficiente restricción a un directorio

Medio de Propagación: Red, Internet

1. **PRODUCTOS AFECTADOS:**

- La versión v1.19.5 de RONDS EPM, una solución de mantenimiento predictivo de equipos.

2. **RESUMEN:**

La explotación exitosa de estas vulnerabilidades podría permitir que un usuario no autorizado filtre las credenciales de inicio de sesión y descargue archivos. En algunas circunstancias, un usuario no autorizado puede usar las credenciales de inicio de sesión para lograr la ejecución remota de código.

3. **DETALLE:**

IMPROPER LIMITATION OF A PATHNAME TO A RESTRICTED DIRECTORY ('PATH TRAVERSAL') CWE-22

RONDS EPM versión 1.19.5 no valida correctamente el parámetro de nombre de archivo, lo que podría permitir que un usuario no autorizado especifique rutas de archivo y descargue archivos.

CVE-2022-2893 ha sido asignado a esta vulnerabilidad. Se ha asignado una puntuación base CVSS v3 de 8.2 (Alta).

EXPOSURE OF SENSITIVE INFORMATION TO AN UNAUTHORIZED ACTOR CWE-200

RONDS EPM versión 1.19.5 tiene una vulnerabilidad en la que una función podría permitir a los usuarios no autenticados filtrar credenciales. En algunas circunstancias, un atacante puede aprovechar esta vulnerabilidad para ejecutar comandos del sistema operativo (OS).

Se ha asignado CVE-2022-3091 a esta vulnerabilidad. Se ha asignado una puntuación base CVSS v3 de 7.5 (Alta).

4. **RECOMENDACIONES:**

- Recomendamos a los usuarios a actualizar el software de RONDS a la versión 1.35.21.

5. **REFERENCIAS:**

- https://nvd.nist.gov/vuln/detail/CVE-2022-3091
- https://nvd.nist.gov/vuln/detail/CVE-2022-2893
- RONDS Equipment Predictive Maintenance Solution | CISA