Alerta de Seguridad

Riesgo de vulnerabilidades IT y OT

31-Mar-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 marzo.

Alertas de Seguridad IT:

- Ransomware MedusaLocker afecta a varios países de Latinoamérica.
- Múltiples vulnerabilidades críticas de ejecución remota en módems 5g Exynos de dispositivos móviles.
- Brecha de seguridad en popular ChatGPT permitía filtrar información personal de usuarios.

Alertas de Seguridad OT/ICS:

- Kaspersky ICS CERT publica su informe H2 2022 sobre amenazas a los sistemas de automatización industrial.
- Fallas de seguridad sin parchear exponen los controladores de bombas de agua a ataques remotos de hackers.

Ransomware MedusaLocker afecta a varios países de Latinoamérica

Tipo de Ataque: Malware

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- Sistemas web en general

2. RESUMEN:

Una nueva variante de MedusaLocker permite vulnerar mecanismos de detección y prevención de amenazas, impactando a varios países de la región.

3. DETALLE:

El ransomware Medusa es una actualización de un malware identificado en 2019, inicialmente utilizado para realizar ataques DDOS pero ahora orientado a la modalidad de cifrado y solicitud de rescate. Entre los medios de propagación que utiliza, se encuentran los ataques de fuerza bruta, phishing, explotación de VPNs, ejecución de código con PowerShell, borrado de instancias con WMI, omisión del control de cuentas de usuario (UAC), explotación del modo seguro, entro otros.

4. RECOMENDACIONES:

Axus ha recopilado información sobre la posible nueva versión de Medusa Locker, que sería la responsable del ataque y ha elaborado una lista comprobada de IOCs relacionados. Se recomienda verificar su bloqueo por parte de las herramientas de seguridad para evitar la afectación de sus operaciones. A continuación, compartimos la compilación de IOCs.

Propagación por WMI

- Archivos QWX.bat, step.bat, step2.bat y n.exe se ejecutan dentro del sistema luego de ser descargados por partes para evadir protección.
- Se crea un nuevo servicio NKBKP y/o NKBKP2.
- Md5:
    - 168447d837fc71deeee9f6c15e22d4f4
    - 0f0da68ff311ce4a8f51a52678d6fdd8
    - 47386ee20a6a94830ee4fa38b419a6f7
    - 19ddac9782acd73f66c5fe040e86ddee
- SHA-256
    - add2850732c42683ee92ba555bbffb88bf5a4eee7c51e24f15a898f2d5aff66b
    - f6586d00b0f766288921d926922c8ad7c2d925e708eacc9925058bd49337db9f
    - dde3c98b6a370fb8d1785f3134a76cb465cd663db20dffe011da57a4de37aa95
    - 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270
    - 89ef8f862ff39fae66ec113c2cab99bfbec737bd4c9613c87b80cf95401adb60
    - add2850732c42683ee92ba555bbffb88bf5a4eee7c51e24f15a898f2d5aff66b
    - f6586d00b0f766288921d926922c8ad7c2d925e708eacc9925058bd49337db9f
    - 26af2222204fca27c0fdabf9eefbfdb638a8a9322b297119f85cce3c708090f0

- SHA-1
    - 80ad29680cb8cecf58d870ee675b155fc616097f
    - eb90356abbeea6f00551afcb25a613b91c3da516
    - ee4575cf9818636781677d63236d3dc65652deab
    - 24ceba1e2951cde8e41939da21c6ba3030fc531d

URLs

- [http://btcfrog[.]com/qr/bitcoinpng[.]php]
- [http://46[.]148[.]235[.]114/cmd.php]

IPs

- 1.3.157[.]61
- 195.123.246[.]138
- 138.124.186[.]221
- 159.223.0[.]9
- 45.146.164[.]141
- 185.220.101[.]35
- 185.220.100[.]249
- 50.80.219[.]149

Múltiples vulnerabilidades críticas de ejecución remota en módems 5G Exynos de dispositivos móviles

Tipo de Ataque: **Explotación de vulnerabilidades**

Medio de Propagación: **Internet**

5. PRODUCTOS AFECTADOS:

- Dispositivos móviles de Samsung, incluidos los de las series S22, A71, A53, A33, A21s, A13, A12, A04
- M33, M13 y M12.
- Dispositivos móviles de Vivo, incluidos los de las series S16, S15, S6, X70, X60 y X30.
- Las series de dispositivos Pixel 6 y Pixel 7 de Google.
- Cualquier vehículo que use el chipset Exynos Auto T5123.
- Dispositivos móviles, puntos de acceso inalámbricos y módems, de marcas como Samsung, Google, LG, Xiaomi, OnePlus, entre otros.

6. RESUMEN:

Se detectaron múltiples vulnerabilidades críticas en dispositivos de Samsung y otras marcas que utilizan el chipset Exynos.

7. DETALLE:

La vulnerabilidad, denominada "Internet to Baseband Remote RCE", permite a los atacantes tomar el control total de los dispositivos y acceder a información privada, así como realizar acciones malintencionadas, simplemente al conectarse a la misma red Wi-Fi que el dispositivo objetivo.

8. RECOMENDACIONES:

Se recomienda a los usuarios que actualicen su software tan pronto como esté disponible para solucionar esta vulnerabilidad, así como evitar conectarse a redes Wi-Fi no confiables y deshabilitar el "hotspot" o punto de acceso en sus dispositivos. También se recomienda a los fabricantes que implementen medidas de seguridad adicionales para prevenir futuras vulnerabilidades.

9. REFERENCIAS:

- https://googleprojectzero.blogspot.com/2023/03/multiple-internet-to-baseband-remote-rce.html
- Product Security Update | Support | Samsung Semiconductor Global

Brecha de seguridad en ChatGPT permitía filtrar información personal de usuarios

Tipo de Ataque: Abuso de inteligencia artificial

Medio de Propagación: Sistemas web en general

1. **PRODUCTOS AFECTADOS:**

- Sistemas en general

2. **RESUMEN:**

Este mes la popular herramienta ChatGPT sufrió su primer gran problema de ciberseguridad. Una brecha de seguridad permitió que usuarios puedan acceder a información personal de al menos 1.2% de los usuarios de ChatGPT Plus.

DETALLE:

El pasado 20 de marzo, OpenAI explicaba que había cerrado momentáneamente ChatGPT para reparar el bug en una librería de código abierto que permitía a algunos usuarios ver los títulos del historial de chat de otros usuarios. Ahora se sabe que la brecha permitiría revelar más datos personales, incluyendo datos de pago y los últimos 4 dígitos de la tarjeta de crédito o débito.

La información que pudo ser afectada incluye:

- Nombre y apellido del usuario
- Dirección de correo electrónico
- Dirección de pago
- Los últimos cuatro dígitos (únicamente) de un número de tarjeta de crédito
- La fecha de vencimiento de la tarjeta de crédito

Según OpenAI, no se ha podido verificar que alguien haya aprovechado las vulnerabilidades para materializar la fuga de información, pero aun cuando así hubiera ocurrido, la información es parcial y nunca corrieron riesgo los números completos de tarjetas de crédito o débito.

3. **REFERENCIAS:**

- La brecha de seguridad de ChatGPT filtró también información personal como los datos de pago, confirma OpenAI (genbeta.com)
- March 20 ChatGPT outage: Here's what happened (openai.com)

Kaspersky ICS CERT publica su informe H2 2022 sobre amenazas a los sistemas de automatización industria

1. RESUMEN:

Kaspersky emitió a principios de mes su informe "Threat Landscape for Industrial Automation Systems: Statistics for H2 2022", el cual es un análisis de las amenazas a los sistemas de automatización industrial durante la segunda mitad del año 2022.

2. DETALLE:

El informe revela que el número total de ataques a sistemas de automatización industrial (IAS) aumentó en un 41% en comparación con la primera mitad del año 2022, y en un 98% en comparación con el mismo periodo del año anterior. También se encontró que el número de sistemas de control industrial (ICS) comprometidos aumentó en un 24% en comparación con la primera mitad del año 2022.

En cuanto a los vectores de ataque, se descubrió que los ataques de phishing continuaron siendo la principal técnica utilizada para comprometer los sistemas de automatización industrial, con un aumento del 32% en comparación con la primera mitad del año 2022. Además, se detectaron más de 2.000 variantes de malware que afectan a los sistemas de automatización industrial, un aumento del 61% en comparación con la primera mitad del año 2022.

El informe también destacó que la industria energética y de suministro de agua y alcantarillado fueron los sectores más afectados por los ataques a los sistemas de automatización industrial en la segunda mitad del año 2022. También se señaló que la mayoría de los ataques se originaron en China, EE. UU., Rusia, India y Ucrania.

3. RECOMENDACIONES:

Se hace hincapié en la importancia de implementar medidas de seguridad adecuadas para proteger los sistemas de automatización industrial.

4. REFERENCIAS:

- Threat landscape for industrial automation systems. Statistics for H2 2022 | Kaspersky ICS CERT

Fallas de seguridad sin parchear exponen los controladores de bombas de agua a ataques remotos de hackers

Medio de Propagación: Red, Internet

1. **PRODUCTOS AFECTADOS:**

- Osprey Pump Controller fabricado por Propump & Controls

2. **RESUMEN:**

Se tiene conocimiento de fallas de seguridad en los controladores de bombas de agua fabricados por la empresa Propump & Controls. Se descubrieron 9 vulnerabilidades categorizadas como críticas y altas en los controladores, que podrían permitir que, entre otras cosas, un atacante remoto tome el control de los sistemas de bombeo de agua.

3. **DETALLE:**

Las vulnerabilidades, que no tienen parches disponibles en este momento, fueron descubiertas por investigadores de la empresa de seguridad cibernética Zero Science Lab. Entre las vulnerabilidades detectadas se encuentran:

Codificación CVE	CVSS v3	Descripción
CVE-2023-28395	8.3	Bypass de autenticación y autorización por algoritmo de generación de token de sesión débil.
CVE-2023-28375	7.5	Fuga de información no autorizada.
CVE-2023-28654	9.8	Uso de contraseña *hard-coded.*
CVE-2023-27886	9.8	Inyección de comandos OS para ejecutar comandos arbitrarios Shell mediante un parámetro HTTP POST.
CVE-2023-27394	9.8	Inyección de comandos OS para ejecutar comandos arbitrarios Shell mediante un parámetro HTTP GET.
CVE-2023-28648	7.5	Neutralización de inputs inapropiada durante la generación de páginas web (ejecución de código HTML/JS).
CVE-2023-28398	9.8	Acceso no autorizado mediante la creación de usuarios nuevos sin validación de credenciales.
CVE-2023-28718	7.1	Cross-Site Request Forgery (CSRF) para la ejecución de acciones vía HTTP sin validaciones.
CVE-2023-28712	8.2	Neutralización de inputs inapropiada durante la generación de páginas web (acceso a sistemas con permisos www-data).

Tabla 1: Lista de vulnerabilidades detectadas

En resumen, las fallas de seguridad en los controladores de bombas de agua fabricados por Propump & Controls representan un grave riesgo para los sistemas de suministro de agua y alcantarillado en todo el mundo.

4. RECOMENDACIONES:

Los administradores de sistemas deben tomar medidas para proteger sus sistemas y presionar a los fabricantes para que proporcionen parches de seguridad para las vulnerabilidades descubiertas.

5. REFERENCIAS:

- Unpatched Security Flaws Expose Water Pump Controllers to Remote Hacker Attacks - SecurityWeek
- https://www.cisa.gov/news-events/ics-advisories/icsa-23-082-06