Alerta de Seguridad

Riesgo de vulnerabilidades IT y OT

31-Mayo-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:

- Aplicación de Android llamada IRecorder - Screen Recorder grabó miles de conversaciones sin autorización de los usuarios.
- Múltiples vulnerabilidades críticas en la interfaz web de ciertos switches de Cisco Small Business.
- Vulnerabilidad en iPhone y iPad permite a los atacantes escapar del entorno de aislamiento seguro de un coprocesador y acceder al kernel del dispositivo.
- Hackers explotaron 7 meses Vulnerabilidad crítica de día cero en dispositivos Email Security Gateway (ESG) de Barracuda.

Alertas de Seguridad OT/ICS:

- Nuevo malware COSMICENERGY, diseñado para interrumpir sistemas críticos en entornos industriales, sector eléctrico.
- El gigante industrial ABB, víctima de ransomware con robo de Información.

Aplicación de Android llamada IRecorder - Screen Recorder grabó miles de conversaciones sin autorización de los usuarios

Tipo de Ataque: Malware

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- Celulares con OS Android

2. RESUMEN:

La aplicación de Android IRecorder – Screen Recorder, comenzó a insertar un troyano de acceso remoto a sus usuarios.

3. DETALLE:

La compañía de ciberseguridad ESET descubrió que la aplicación tenía un código malicioso oculto que activaba el micrófono de los usuarios y grababa muestras de audio cada 15 minutos, enviándolas a un servidor privado. La aplicación pasó la prueba de confianza de Google y estuvo disponible en la tienda oficial durante 11 meses hasta que una actualización la convirtió en un malware, al insertar un troyano de acceso remoto (RAT) llamado ahMYth, que tiene la facultad de extraer imágenes, videos y archivos para reenviarlos sin que el usuario se dé cuenta.

Aunque la presencia del troyano fue reportada en octubre de 2022, Google no emitió ninguna alerta sobre la aplicación y continuó recibiendo actualizaciones hasta febrero de 2022. Finalmente, en mayo de 2023, Google retiró la aplicación de su tienda después de acumular más de 50 mil descargas. ESET advierte que el comportamiento malicioso de la aplicación indica la posibilidad de estar involucrada en una campaña de espionaje, aunque no hay pruebas suficientes para atribuirlo a una campaña en particular.

4. RECOMENDACIONES:

- Se debe tener precaución al instalar aplicaciones de la tienda de Google Play y verificar regularmente los permisos que solicitan.
- Activar la función de hibernación en Android 11, que suspende los permisos de ejecución de las aplicaciones cuando no se utilizan durante un tiempo determinado, como medida de seguridad.
- Instalar solo aplicaciones de confianza y estar atento a posibles riesgos de seguridad para prevenir el robo de información personal.

5. REFERENCIAS:

- IRecorder: esta App de Android grabó miles de conversaciones sin autorización | WIRED

Múltiples vulnerabilidades críticas en la interfaz web de ciertos switches de Cisco Small Business

Tipo de Ataque: Explotación de vulnerabilidades

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**

- 250 Series Smart Switches
- 350 Series Managed Switches
- 350X Series Stackable Managed Switches
- 550X Series Stackable Managed Switches
- Business 250 Series Smart Switches
- Business 350 Series Managed Switches
- Small Business 200 Series Smart Switches
- Small Business 300 Series Managed Switches
- Small Business 500 Series Stackable Managed Switches

2. **RESUMEN:**

Estas vulnerabilidades podrían permitir a un atacante remoto y no autenticado causar una denegación de servicio (DoS) o ejecutar código arbitrario con privilegios de root en un dispositivo afectado. Las vulnerabilidades se deben a una validación inadecuada de las solicitudes enviadas a la interfaz web.

3. **DETALLE:**

Las vulnerabilidades afectan a varios modelos de switches de la serie Cisco Small Business, incluidos los switches inteligentes de la serie 250, los switches gestionados de la serie 350, los switches apilables gestionados de la serie 350X y 550X, y otros modelos. Cisco ha lanzado actualizaciones de software para abordar estas vulnerabilidades y no hay soluciones alternativas disponibles.

Las vulnerabilidades específicas incluyen desbordamiento de búfer de stack y de búfer de heap, así como una vulnerabilidad de lectura de configuración no autenticada. Estas vulnerabilidades podrían permitir que un atacante ejecute código arbitrario o cause una denegación de servicio en un dispositivo afectado.

Cisco recomienda a los clientes que posean contratos de servicio obtener las correcciones de seguridad a través de sus canales habituales de actualización. Aquellos clientes que no tengan un contrato de servicio pueden ponerse en contacto con el Centro de Asistencia Técnica (TAC) de Cisco para obtener las actualizaciones necesarias.

Además, se menciona que se ha publicado código de explotación de prueba de concepto para estas vulnerabilidades, pero no se tiene conocimiento de ningún uso malicioso de las mismas.

4. **RECOMENDACIONES:**

Actualizar a las versiones de software corregidas para proteger sus dispositivos contra estas vulnerabilidades críticas.

5. **REFERENCIAS:**

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv

Vulnerabilidad en iPhone y iPad permite a los atacantes escapar del entorno de aislamiento seguro de un coprocesador y acceder al kernel del dispositivo

Tipo de Ataque: Explotación de vulnerabilidades

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**

- Dispositivos con iOS 16.5
- Dispositivos con iPadOS 16.5

2. **RESUMEN:**

Una nueva vulnerabilidad descubierta en iOS 16.5 y iPadOS 16.5 que afecta a los dispositivos iPhone y iPad. La vulnerabilidad, denominada ColdInvite (CVE-2023-27930), permite a los atacantes escapar del entorno de aislamiento seguro de un coprocesador y acceder al kernel del dispositivo. Esto podría permitir ataques más sofisticados y potencialmente peligrosos.

3. **DETALLE:**

Apple ya había lanzado una actualización anterior, iOS 15.6.1, para mitigar una vulnerabilidad similar llamada ColdIntro (CVE-2022-32894), pero no abordó completamente el problema del coprocesador subyacente. Sin embargo, se sospecha que Apple ha solucionado este problema al reescribir gran parte del software del coprocesador en versiones posteriores del sistema operativo.

Durante el análisis de ColdIntro, los investigadores descubrieron la vulnerabilidad ColdInvite, que permite a los atacantes escapar de un coprocesador y corromper la memoria del Procesador de Aplicaciones (AP). Esta vulnerabilidad afecta a los modelos de iPhone 12 y posteriores.

Apple ha parcheado la vulnerabilidad en iOS 16.5 y iPadOS 16.5 en respuesta al informe de Jamf Threat Labs. Sin embargo, los investigadores advierten que este tipo de ataques y vulnerabilidades de escape de coprocesadores podrían continuar en el futuro.

Aunque esta noticia puede generar preocupación entre los propietarios de iPhone y iPad, Apple ha tomado medidas proactivas para mejorar la seguridad de sus dispositivos con las actualizaciones Rapid Security Response.

4. **RECOMENDACIÓN:**

Es importante destacar que los parches de seguridad de Rapid Security Response se agregan posteriormente a las actualizaciones de iOS, lo que demuestra el compromiso de Apple con la seguridad. Sin embargo, los usuarios finales aún pueden ser el eslabón débil, por lo que se recomienda a los propietarios de iPhone y iPad a mantener sus dispositivos actualizados de manera más proactiva que nunca.

5. **REFERENCIAS:**

- https://www.forbes.com/sites/gordonkelly/2023/05/22/apple-ios-165-new-attack-type-iphone-ipad-update/?sh=7f8cd0993dbd

Hackers explotaron 7 meses Vulnerabilidad crítica de día cero en dispositivos Email Security Gateway (ESG) de Barracuda

Medio de Propagación: Red, Internet

1. **PRODUCTOS AFECTADOS:**
   - Dispositivo Email Scurity Gateway (ESG)
2. **RESUMEN:**

Barracuda, una empresa de seguridad empresarial, reveló que los piratas informáticos explotaron una falla de día cero en sus dispositivos Email Security Gateway (ESG) durante aproximadamente siete meses antes de su descubrimiento.

3. **DETALLE:**

La vulnerabilidad, identificada como CVE-2023-2868, permitió a atacantes remotos ejecutar código en instalaciones vulnerables. Barracuda lanzó parches el 20 y 21 de mayo para solucionar el problema. La falla afectó a las versiones de ESG 5.1.3.001 a 9.2.0.006. Se descubrieron cepas de malware denominadas SALTWATER, SEASPY y SEASIDE en relación con la explotación de la vulnerabilidad, y se encontraron pruebas de exfiltración de datos en algunos dispositivos afectados. La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA, por sus siglas en inglés) agregó el error a su catálogo de Vulnerabilidades Explotadas Conocidas e instó a las agencias federales a aplicar las correcciones antes del 16 de junio de 2023. Barracuda se comunicó directamente con las organizaciones afectadas y advirtió que es posible que se descubran más usuarios afectados a medida que el continúa la investigación. Los ataques no se han atribuido a un actor o grupo de amenazas específico.

4. **RECOMENDACIONES**
   - Asegúrese de que su dispositivo ESG reciba y aplique actualizaciones, definiciones y parches de seguridad de Barracuda. Comuníquese con el soporte de Barracuda (support@barracuda.com) para validar si el dispositivo está actualizado.
   - Suspenda el uso del dispositivo ESG comprometido y comuníquese con el soporte de Barracuda (support@barracuda.com) para obtener un nuevo dispositivo virtual o de hardware ESG.
   - Rote cualquier credencial aplicable conectada al dispositivo ESG:
     - Cualquier LDAP/AD conectado
     - Barracuda Cloud Control
     - Servidor FTP
     - PYME
     - Cualquier certificado TLS privado
   - Revise sus registros de red para cualquiera de los IOC enumerados a continuación y cualquier IP desconocida.

5. **REFERENCIAS:**

- Industrial Giant ABB Confirms Ransomware Attack, Data Theft - SecurityWeek
- Multinational tech firm ABB hit by Black Basta ransomware attack (bleepingcomputer.com)

Nuevo malware COSMICENERGY, diseñado para interrumpir sistemas críticos en entornos industriales, sector eléctrico.

Tipo de Ataque: Malware

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**

- Sistemas críticos en entornos industriales.

1. RESUMEN:

Se ha descubierto un nuevo malware llamado COSMICENERGY, diseñado específicamente para penetrar e interrumpir sistemas críticos en entornos industrials.

2. DETALLE:

El malware se dirige a dispositivos que utilizan el protocolo IEC 60870-5-104 (IEC-104), comúnmente utilizado en operaciones de transmisión y distribución eléctrica en Europa, Medio Oriente y Asia. COSMICENERGY comparte similitudes con otros programas maliciosos como Stuxnet e Industroyer, conocidos por sabotear sistemas críticos. Se cree que el malware puede haber sido desarrollado como una herramienta de equipo rojo por la empresa de telecomunicaciones rusa Rostelecom-Solar para simular escenarios de interrupción del suministro eléctrico. El malware utiliza dos componentes, PIEHOP y LIGHTWORK, para enviar comandos a los equipos industriales y causar cortes de energía. En particular, COSMICENERGY requiere un reconocimiento interno por parte del operador para identificar los dispositivos objetivo. Su descubrimiento antes de ser utilizado activamente en ataques del mundo real destaca el panorama de amenazas en evolución en entornos de tecnología operativa (OT).

3. RECOMENDACIONES:

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

4. REFERENCIAS:

- https://thehackernews.com/2023/05/new-cosmicenergy-malware-exploits-ics.html#:~:text=New%20COSMICENERGY%20Malware%20Exploits%20ICS%20Protocol%20to%20Sabotage%20Power%20Grids,-%EE%A0%82May%2026&text=A%20new%20strain%20of%20malicious,industrial%20environments%20has%20been%20unearthed.

El gigante industrial ABB, víctima de ransomware con Robo de Información

Medio de Propagación: Red, Internet

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de información
2. **RESUMEN:**

El gigante industrial suizo ABB ha confirmado que recientemente fue objeto de un ataque de ransomware en el que los ciberdelincuentes robaron algunos datos.

3. **DETALLE:**

La compañía ha publicado un comunicado de prensa y preguntas frecuentes sobre el incidente, pero ha ocultado muchos detalles debido a una investigación policial en curso. ABB ha determinado que un tercero no autorizado accedió a sus sistemas, implementó un ransomware no autopropagante y filtró ciertos datos. Según los informes, el malware se implementó en una cantidad limitada de servidores y puntos finales y no se propagó automáticamente por correo electrónico o la red local. ABB asegura que sus servicios y sistemas clave estén operativos, que las fábricas están funcionando y que siguen sirviendo a los clientes. La empresa está restaurando los servicios afectados restantes, mejorando la seguridad del sistema y evaluando la naturaleza y el alcance de los datos afectados. ABB ha notificado a los clientes que no hay evidencia de un impacto directo en sus sistemas y ninguna indicación de que no sea seguro conectarse a los sistemas de ABB.

Diversas fuentes sugieren que el ataque fue perpetrado por el grupo Black Basta y que sí habría afectado las operaciones y las fábricas. Los informes sugieren que ABB pagó el rescate, lo que podría explicar por qué no se los nombró en el sitio web de fugas del grupo de ransomware.

4. **REFERENCIAS:**

- Industrial Giant ABB Confirms Ransomware Attack, Data Theft - SecurityWeek
- Multinational tech firm ABB hit by Black Basta ransomware attack (bleepingcomputer.com)