Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

8-Nov-2022

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 Octubre.

Alertas de Seguridad IT:

- Guía sobre vulnerabilidades de día cero en Microsoft Exchange Server.
- Nuevos Exploits aprovechan vulnerabilidades Críticas y Altas de varios productos.
- El Ransomware Venus ataca a servicios RDP expuestos en todo el mundo.

Alertas de Seguridad OT/ICS:

- Múltiples Vulnerabilidades Críticas en Procesadores Snapdragon.
- Vulnerabilidad Crítica en servidores Siemens Siveillance Video Mobile.

Guía sobre vulnerabilidades de día cero en Microsoft Exchange Server

Tipo de Ataque: **Explotación de vulnerabilidades conocidas**

Medio de Propagación: **Red, Internet**

1. PRODUCTOS AFECTADOS:

- Microsoft Exchange Server (**Nota**: Microsoft Online no está afectado)

2. RESUMEN:

Dos vulnerabilidades de día cero fueron notificadas para Microsoft Exchange Server 2013, 2016 y 2019. Mediante la explotación de estas vulnerabilidades los atacantes pueden tomar el control del sistema.

3. DETALLE:

Microsoft ha publicado una Guía para el cliente sobre vulnerabilidades de día cero notificadas en Microsoft Exchange Server. Según la publicación del blog, "Microsoft es consciente de los ataques dirigidos limitados que utilizan las dos vulnerabilidades para ingresar a los sistemas de los usuarios". Las dos vulnerabilidades son CVE-2022-41040 y CVE-2022-41082, que afectan a las instalaciones on-premise de Microsoft Exchange Server 2013, 2016 y 2019. Un atacante podría explotar estas vulnerabilidades para tomar el control de un sistema afectado.

La lista de vulnerabilidades es la siguiente:

CVE ID	Fabricante	Producto	CVSS v3	Descripción
CVE-2022-41040	Microsoft	Exchange Server	8.8	Elevación de privilegios en Microsoft Exchange Server
CVE-2022-41082	Microsoft	Exchange Server	8.8	Vulnerabilidad de ejecución de código remoto para Microsoft Exchange Server

Tabla 1: Lista de vulnerabilidades Microsoft Exchange

4. RECOMENDACIONES:

- Se recomienda a los usuarios y administradores a aplicar las acciones de mitigación necesarias hasta que los parches estén disponibles.

5. REFERENCIAS:

- https://www.cisa.gov/uscert/ncas/current-activity/2022/09/30/microsoft-releases-guidance-zero-day-vulnerabilities-microsoft
- https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

Nuevos exploits aprovechan vulnerabilidades Críticas y Altas de varios productos

Tipo de Ataque: Explotación de vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. PRODUCTOS AFECTADOS:

- Exchange server
- Fortinet, múltiples productos
- Cisco AnyConnect Secure
- Otros

2. RESUMEN:

Se detectaron múltiples vulnerabilidades críticas y altas de varios productos de los principales fabricantes de soluciones de tecnología, entre ellos: Microsoft, Fortinet, Cisco, GIGABYTE, etc. Estas vulnerabilidades pueden ser aprovechadas mediante software “listos para usar” (ready-to-use).

3. DETALLE:

En el último mes, se han estado explotando diversas vulnerabilidades críticas y altas usando módulos de software listos para usar (exploits), aumentando el riesgo de estas vulnerabilidades.

A continuación listamos los productos afectados y las respectivas vulnerabilidades.

Lista de vulnerabilidades:

CVE ID	Fabricante	Producto	CVSS v3	Descripción
CVE-2022-40684	Fortinet	Múltiples productos	9.8	Vulnerabilidad de omisión de autenticación de múltiples productos de Fortinet.
CVE-2022-41352	Zimbra	Collaboration (ZCS)	9.8	Vulnerabilidad de carga de archivos arbitrarios de Zimbra Collaboration (ZCS).
CVE-2022-36804	Atlassian	Bitbucket Server y Data Center	8.8	Vulnerabilidad de inyección de comandos de Atlassian Bitbucket Server y Data Center.
CVE-2022-41082	Microsoft	Exchange Server	8.8	Vulnerabilidad de ejecución remota de código de Microsoft Exchange Server.
CVE-2022-41040	Microsoft	Exchange Server	8.8	Vulnerabilidad de falsificación de solicitudes del lado del servidor de Microsoft Exchange Server.
CVE-2022-41033	Microsoft	Windows COM+ Event System Service	7.8	Vulnerabilidad de escalada de privilegios del servicio del sistema de eventos COM+ de Microsoft Windows.
CVE-2021-3493	Linux	Kernel	7.8	Vulnerabilidad de escalada de privilegios del Kernel de Linux.

CVE-2020-3433	Cisco	AnyConnect Secure	7.8	Cisco AnyConnect Secure Mobility Client para Windows. Vulnerabilidad de secuestro de DL.
CVE-2020-3153	Cisco	AnyConnect Secure	6.5	Cisco AnyConnect Secure Mobility Client para Windows. Vulnerabilidad de ruta de búsqueda no controlada.
CVE-2018-19323	GIGABYTE	Múltiples productos	9.8	Vulnerabilidad de escalada de privilegios de múltiples productos de GIGABYTE.
CVE-2018-19322	GIGABYTE	Múltiples productos	7.8	Vulnerabilidad de ejecución de código de múltiples productos de GIGABYTE.
CVE-2018-19321	GIGABYTE	Múltiples productos	7.8	Vulnerabilidad de escalada de privilegios de múltiples productos de GIGABYTE.
CVE-2018-19320	GIGABYTE	Múltiples productos	7.8	Vulnerabilidad no especificada de varios productos de GIGABYTE.

Tabla 2: Lista de vulnerabilidades detectadas

Entre estas vulnerabilidades destaca la CVE-2022-40684, que es una omisión de autenticación en FortiOS, FortiProxy y FortiSwitchManager. La vulnerabilidad ya ha sido clasificada como crítica (9.8 en CVSS v3). Ahora con el exploit circulando, se vuelve aún más probable que intenten explotarla atacantes sin un mayor nivel técnico.

4. RECOMENDACIONES:

- Aplicar de manera urgente las últimas actualizaciones de seguridad de cada producto.

5. REFERENCIAS:

- https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
- https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
- https://jira.atlassian.com/browse/BSERV-13438
- https://www.fortiguard.com/psirt/FG-IR-22-377
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41033
- https://wiki.zimbra.com/wiki/Security_Center
- https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=7c03e2cda4a584cadc398e8f6641ca9988a39d52
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ac-win-path-traverse-qO4HWBsj
- https://www.gigabyte.com/Support/Security/1801

El Ransomware Venus ataca a servicios RDP expuestos en todo el mundo

Tipo de Ataque: Ransomware

Medio de Propagación: Vulnerabilidades conocidas del protocolo RDP de servidores Windows

1. PRODUCTOS AFECTADOS:

- Servicios RDP expuestos a internet

2. RESUMEN:

Desde agosto de este año, los actores de amenaza detrás del Ransomware Venus están atacando en todo el mundo a los servicios de escritorio remoto (RDP), viéndolo como una puerta de entrada en sus ataques. La poca robustez de las credenciales usadas por muchos usuarios y las insuficientes defensas en muchas infraestructuras permiten que ataques por "fuerza bruta" puedan vulnerar tu dispositivo.

3. DETALLE:

Cuando se ejecuta, el ransomware Venus intentará finalizar 39 procesos asociados con servidores de bases de datos y aplicaciones de Microsoft Office. Entre ellos:

> sqlagent.exe, sqlbrowser.exe, sqlservr.exe, sqlwriter.exe, oracle.exe, ocssd.exe, dbsnmp.exe, infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, sqlservr.exe, thebat64.exe, thunderbird.exe, winword.exe, wordpad.exe

El ransomware también eliminará los registros de eventos (logs), los volúmenes de instantánea (Volume Shadow Copy) y deshabilitará la prevención de ejecución de datos (Data Execution Prevention) mediante el siguiente comando:

> wbadmin delete catalog -quiet && vssadmin.exe delete shadows /all /quiet && bcdedit.exe /set {current} nx AlwaysOff && wmic SHADOWCOPY DELETE

Al cifrar archivos, el ransomware agregará la extensión.venus, como se muestra a continuación. Por ejemplo, un archivo llamado test.jpg se cifraría y cambiaría de nombre test.jpg.venus.

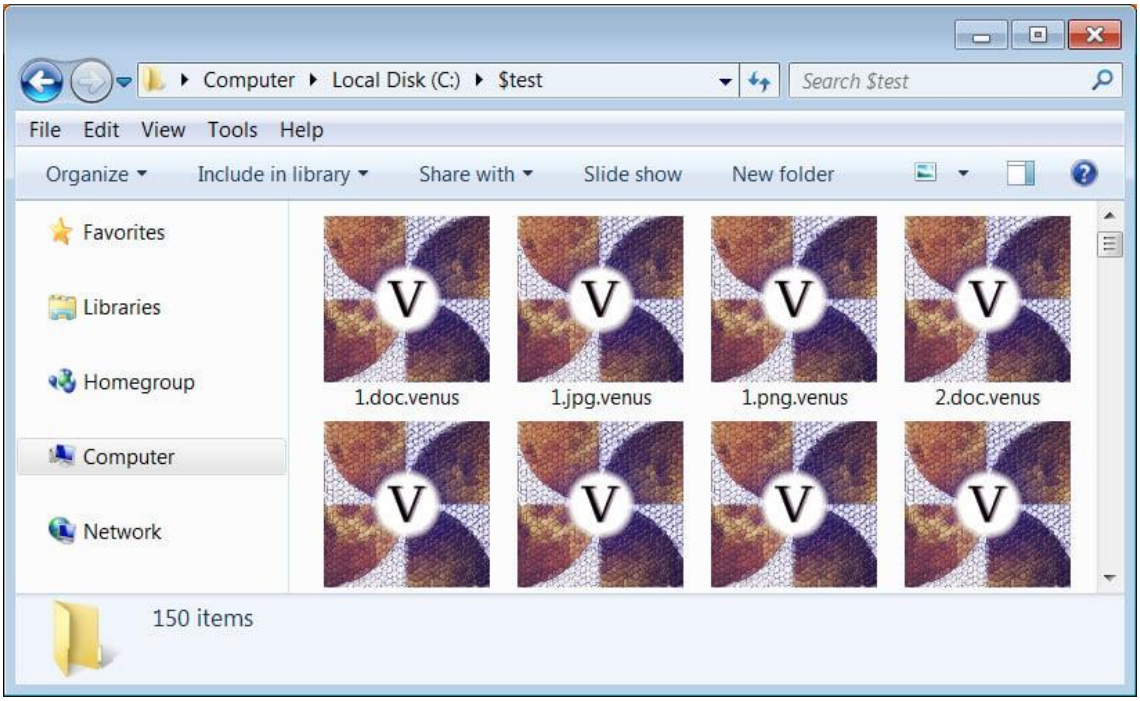

Figura 1: Archivos cifrados por el Ransomware Venus

El ransomware creará una nota de rescate en formato .HTA en la carpeta %Temp% que se mostrará automáticamente cuando el ransomware termine de cifrar el dispositivo.

Como se puede ver a continuación, este ransomware se llama a sí mismo "Venus" y comparte una dirección TOX y una dirección de correo electrónico que se pueden usar para contactar al atacante para negociar el pago de un rescate. Al final de la nota de rescate hay un blob codificado en base64, que probablemente sea la clave de descifrado encriptada.

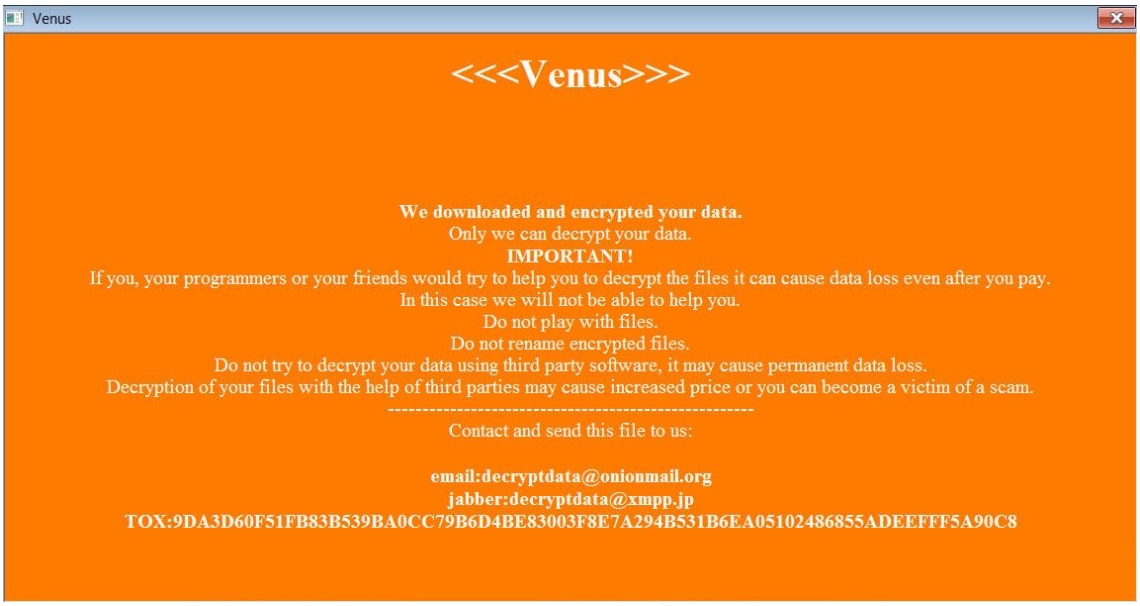

Figura 2: Mensaje Ransomware Venus

4. RECOMENDACIONES:

- Deshabilitar servicios con protocolo RDP que estén expuestos a internet. No es suficiente cambiar el puerto por defecto, los atacantes buscan este protocolo en otros puertos también. De ser muy necesario, se puede usar el protocolo RDP dentro de un canal protegido por VPN, que a su vez tenga múltiple factor de autenticación.

5. REFERENCIAS:

- Venus Ransomware targets publicly exposed Remote Desktop services (bleepingcomputer.com)
- VirusTotal - File - 6d8e2d8f6aeb0f4512a53fe83b2ef7699513ebaff31735675f46d1beea3a8e05

Múltiples Vulnerabilidades Críticas en Procesadores Snapdragon

Tipo de Ataque: Buffer overflow, buffer overread y otros abusos de límites de memoria

Medio de Propagación: Ataque programático que usa cualquier medio de difusión de software malicioso

1. PRODUCTOS AFECTADOS:

- Snapdragon Industrial IOT, Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking.

2. RESUMEN:

Se publicaron una serie de vulnerabilidades críticas de procesadores Snapdragon, los cuales presentaban una debilidad a los ataques de desbordamiento de buffer. Este tipo de ataques podrían ser ejecutados sin la necesidad de interactuar con el usuario. No obstante, ya han sido publicados los respectivos parches para estos dispositivos.

3. DETALLE:

El pasado 19 de octubre, Qualcomm Technologies publicó una serie de vulnerabilidades críticas (sin requerir interacción con el usuario) que representan una debilidad de estos sistemas frente a ataques de desbordamiento de buffer relacionados al abuso de los límites de memoria en variables específicas. Para hacer efectivo este tipo de ataques no es necesaria la interacción con el usuario, un software malicioso debe poder interactuar con el sistema operativo soportado por el procesador Snapdragon.

El fabricante ya lanzó parches para las vulnerabilidades detectadas en los dispositivos afectados y estará incluyéndolos en los siguientes dispositivos comercializados.

Esta tabla enumera vulnerabilidades de seguridad de alto impacto.

CVE ID	CVSS v3	Área
CVE-2022-25748	9.8	WLAN Firmware
CVE-2022-25718	9.1	Network Service
CVE-2022-25661	8.4	KERNEL
CVE-2022-33210	8.4	Multimedia
CVE-2022-25719	8.2	Network Service
CVE-2022-25660	7.8	KERNEL
CVE-2022-25736	7.5	WLAN Firmware
CVE-2022-25749	7.5	WLAN Firmware
CVE-2022-25687	7.3	Video

Tabla 3: Lista de vulnerabilidades de seguridad de alto impacto

4. RECOMENDACIONES:

- Mantener actualizado el software, incluyendo el sistema operativo, con los últimos parches de seguridad.

5. REFERENCIAS:

- https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2022-bulletin.html

Vulnerabilidad Crítica en servidores Siemens Siveillance Video Mobile

Tipo de Ataque: Toma de control remotamente, baja complejidad

Medio de Propagación: Varios

1. PRODUCTOS AFECTADOS:

- Siveillance Video 2022 R2, todas las versiones menores a V22.2a

2. RESUMEN:

Se descubrió una vulnerabilidad crítica en los servidores de Siemens Siveillance Video Mobile. Cuando se intenta acceder a un recurso o ejecutar una acción, este software realiza una comprobación de autorización al usuario. Sin embargo, este no realiza de manera correcta la comprobación, permitiendo a los atacantes eludir las restricciones previstas.

3. DETALLE:

La explotación de esta vulnerabilidad puede permitir a un atacante remoto, sin necesidad de credenciales válidas, ingresar a una aplicación con alto impacto en la integridad y la confidencialidad. El componente del servidor móvil de las aplicaciones afectadas maneja incorrectamente el inicio de sesión para las cuentas de Active Directory que forman parte del grupo de Administradores.

CVE ID	Fabricante	Producto	CVSS v3	Descripción
CVE-2022-43400	Siemens	Siveillance Video Mobile Server	9.4	Autorización incorrecta

Tabla 4: Clasificación Vulnerabilidad Siemens

4. RECOMENDACIONES:

- Aplicar las últimas actualizaciones de seguridad de este producto: Mobile Server Installer (Vulnerability Hotfix), disponible en el portal de soporte de Siemens Industrial.
- Habilite la función " Servers > Mobile Servers > Deny the built-in Administrators role access to the mobile servers" para todos los servidores móviles configurados.

5. REFERENCIAS:

- https://cert-portal.siemens.com/productcert/pdf/ssa-640732.pdf
- https://nvd.nist.gov/vuln/detail/CVE-2022-43400
- https://www.cisa.gov/uscert/ics/advisories/icsa-22-298-03