BOLETÍN DE CIBERSEGURIDAD

MARZO 2024

ÍNDICE

NOTICIAS INTERNACIONALES

URGENTE: SE ENCONTRÓ UNA PUERTA TRASERA SECRETA EN LA BIBLIOTECA XZ UTILS QUE AFECTA A LAS PRINCIPALES DISTRIBUCIONES DE LINUX.

Se indico que dos versiones de una conocida biblioteca de compresión de datos, XZ Utils (previamente conocida como LZMA Utils), contenían una puerta trasera con código malicioso diseñada para permitir acceso remoto no autorizado.

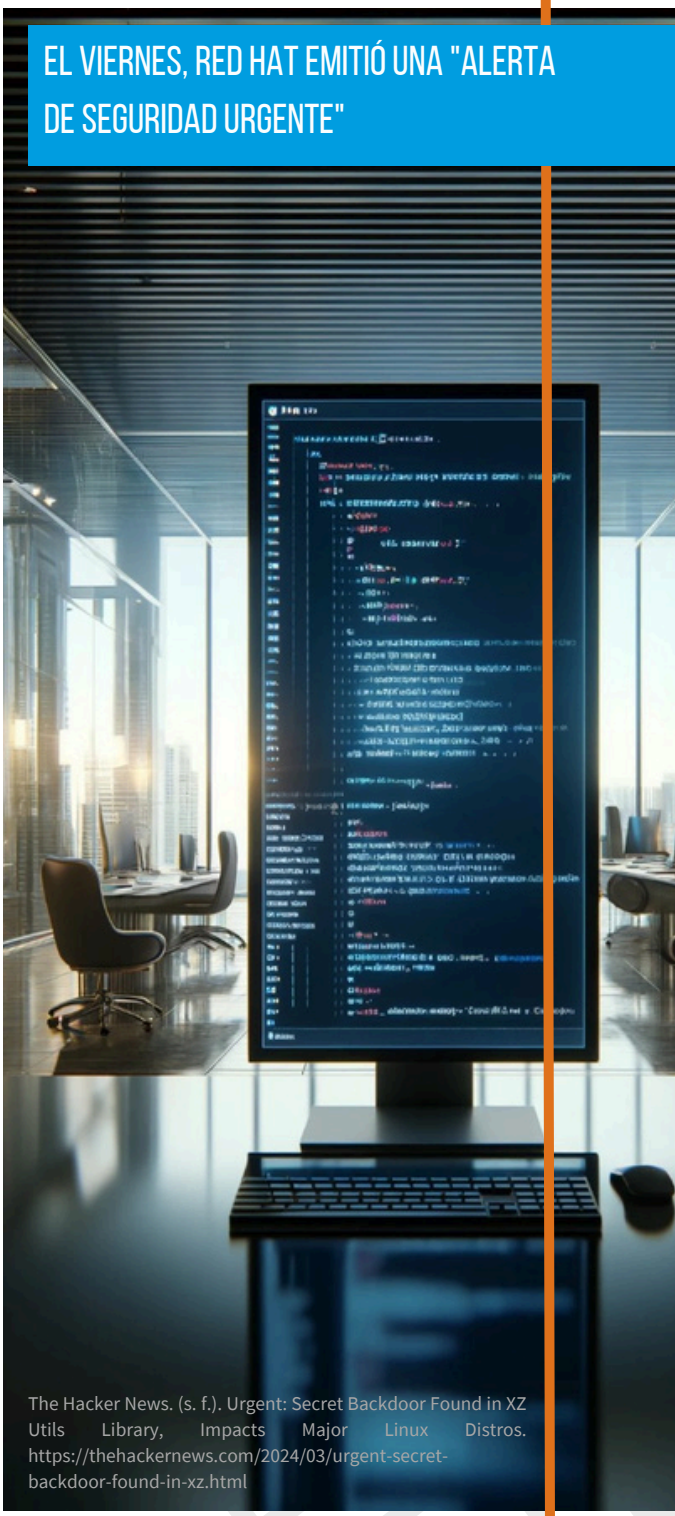
El incidente en la cadena de suministro de software, identificado como CVE-2024-3094, posee una puntuación CVSS de 10,0, lo que denota una severidad máxima. Esta vulnerabilidad afecta a las versiones 5.6.0 y 5.6.1 de XZ Utils, lanzadas el 24 de febrero y el 9 de marzo, respectivamente.

Según un aviso de la filial de IBM, "a través de una serie de complicadas técnicas de ofuscación, el proceso de construcción de liblzma extrae un archivo objeto predefinido de un archivo de prueba camuflado presente en el código fuente, que luego se emplea para modificar funciones específicas dentro del código de liblzma".
"Como resultado de esto, se genera una versión alterada de la biblioteca liblzma que puede ser empleada por cualquier software que esté vinculado a ella, interfiriendo y alterando la interacción de datos con dicha biblioteca".

Concretamente, el código maligno integrado en el software está diseñado para interferir con el proceso del demonio sshd utilizado por SSH (Secure Shell) a través del paquete de software systemd, potencialmente permitiendo que un actor de amenazas supere la autenticación sshd y acceda de forma no autorizada al sistema de manera remota "bajo circunstancias apropiadas".

"El propósito final de esta puerta trasera maliciosa introducida por CVE-2024-3094 es inyectar código en el servidor OpenSSH (SSHD) en ejecución en la máquina objetivo y permitir que atacantes remotos específicos (que posean una clave privada específica) envíen cargas útiles de datos arbitrarios a través de SSH que se ejecutarán antes del proceso de autenticación, efectivamente tomando el control total de la máquina objetivo", mencionó JFrog.

EL VIERNES, RED HAT EMITIÓ UNA "ALERTA DE SEGURIDAD URGENTE"



The Hacker News. (s. f.). Urgent: Secret Backdoor Found in XZ Utils Library, Impacts Major Linux Distros. https://thehackernews.com/2024/03/urgent-secret-backdoor-found-in-xz.html

Andrés Freund, investigador de seguridad en Microsoft, se le atribuye el mérito de descubrir e informar sobre el problema el viernes. Se dice que el código malicioso, altamente enmascarado, fue introducido durante una serie de cuatro confirmaciones en el Proyecto Tukaani en GitHub por un usuario identificado como Jia Tan (JiaT75).

Redaccion. (2024, 28 febrero). Sophos Partner Care, nuevo servicio del fabricante de ciberseguridad - MuyPymes. MuyPymes. https://www.muypymes.com/2024/02/28/sophos-partner-care-servicio-fabricante-ciberseguridad

SOPHOS PARTNER CARE ES UN NUEVO SERVICIO DE ATENCIÓN PERSONALIZADA PARA SOCIOS CORPORATIVOS QUE NOS LO PRESENTARON EN MUYCANAL

PHOBOS RANSOMWARE SE DIRIGE AGRESIVAMENTE A LA INFRAESTRUCTURA CRÍTICA DE EE. UU.

Las agencias de inteligencia y ciberseguridad de los Estados Unidos han emitido una advertencia sobre los ataques de ransomware Phobos dirigidos a entidades gubernamentales y de infraestructura crítica. Describen las tácticas y técnicas utilizadas por los actores de amenazas para implementar el malware de cifrado de archivos.

Según el informe gubernamental, estructurado como un modelo de ransomware como servicio (RaaS), los operadores del ransomware Phobos han apuntado a entidades como gobiernos municipales y de condado, servicios de emergencia, educación, atención médica pública e infraestructura crítica, logrando recaudar varios millones de dólares estadounidenses en rescates.

La advertencia proviene de la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA), el FBI y el Centro de Análisis e Intercambio de Información Multiestatal (MS-ISAC).

Desde mayo de 2019, se han identificado múltiples variantes del ransomware Phobos, incluidas Eking, Eight, Elbie, Devos, Faust y Backmydata. En un desarrollo reciente, Cisco Talos reveló que los operadores de ransomware 8Base están utilizando una variante del ransomware Phobos para sus ataques con motivación financiera.

Hay indicios que sugieren que Phobos está probablemente gestionado de cerca por una autoridad central que controla la clave privada de descifrado del ransomware.

PHOBOS RANSOMWARE SE DIRIGE AGRESIVAMENTE A LA INFRAESTRUCTURA CRÍTICA DE EE. UU.

Las cadenas de ataque que involucran esta cepa de ransomware generalmente comienzan con el phishing como vector de acceso inicial, mediante el cual se envían cargas útiles sigilosas como SmokeLoader. Alternativamente, se aprovechan redes vulnerables buscando servicios RDP expuestos y explotándolos mediante ataques de fuerza bruta.

Después de una intrusión digital exitosa, los actores de amenazas suelen dejar caer herramientas adicionales de acceso remoto, emplear técnicas de inyección de procesos para ejecutar código malicioso y evadir la detección, así como realizar modificaciones en el Registro de Windows para mantener la persistencia dentro de los entornos comprometidos.

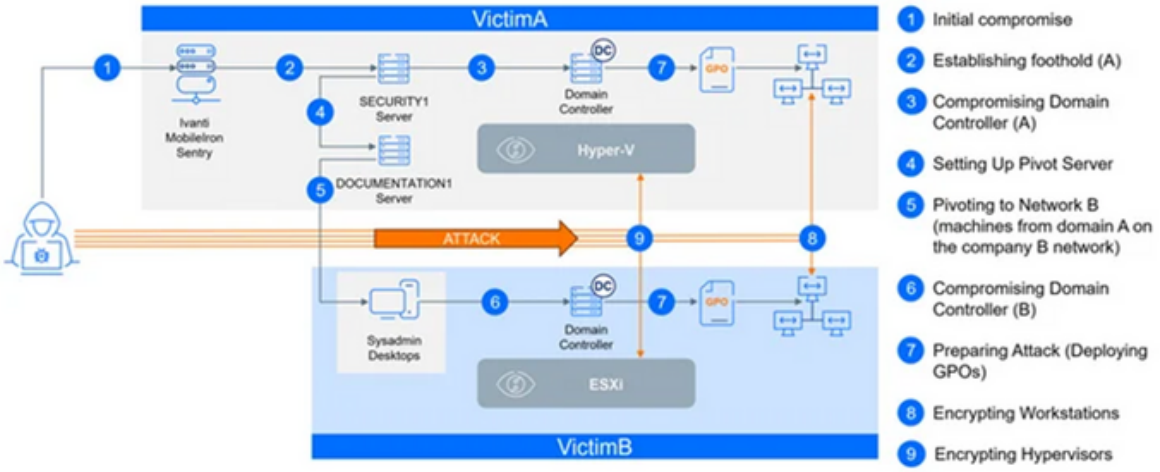
"Además, se ha observado que los actores de Phobos utilizan funciones API integradas de Windows para robar tokens, eludir los controles de acceso y crear nuevos procesos para escalar privilegios aprovechando el proceso SeDebugPrivilege", mencionaron las agencias. "Los actores de Phobos intentan autenticarse utilizando hashes de contraseñas almacenados en caché en las máquinas víctimas hasta que alcanzan el acceso de administrador de dominio".

Se sabe que el grupo de delitos electrónicos utiliza herramientas de código abierto como Bloodhound y Sharphound para enumerar el directorio activo. La exfiltración de archivos se lleva a cabo mediante WinSCP y Mega.io, después de lo cual se eliminan las instantáneas de volumen en un intento de dificultar la recuperación.

Esta divulgación coincide con el detalle de un ataque de ransomware meticulosamente coordinado por Bitdefender, que afecta a dos empresas distintas al mismo tiempo. El ataque, descrito como sincronizado y multifacético, se ha atribuido a un actor de ransomware llamado CACTUS.

"CACTUS continuó infiltrándose en la red de una organización, implantando varios tipos de herramientas de acceso remoto y túneles a través de diferentes servidores", explicó Martin Zugec, director de soluciones técnicas de Bitdefender, en un informe publicado la semana pasada.

"Cuando identificaron una oportunidad de moverse a otra empresa, pausaron momentáneamente su operación para infiltrarse en la otra red. Ambas empresas son parte del mismo grupo, pero operan de forma independiente, manteniendo redes y dominios separados sin ninguna relación de confianza establecida".



PHOBOS RANSOMWARE SE DIRIGE AGRESIVAMENTE A LA INFRAESTRUCTURA CRÍTICA DE EE. UU.

El ataque también se destaca por dirigirse a la infraestructura de virtualización de la empresa anónima, lo que sugiere que los actores de CACTUS han expandido su enfoque más allá de los hosts de Windows para atacar los hosts Hyper-V y VMware ESXi.

Además, aprovechó una falla de seguridad crítica (CVE-2023-38035, con una puntuación CVSS de 9.8) en un servidor Ivanti Sentry expuesto a Internet menos de 24 horas después de su divulgación inicial en agosto de 2023, lo que nuevamente resalta el uso rápido y oportunista de vulnerabilidades recientemente publicadas como una táctica.

El ransomware sigue siendo una fuente importante de ingresos para los actores de amenazas con motivación financiera, y las demandas iniciales de ransomware alcanzarán un promedio de 600 000 dólares en 2023, un aumento del 20 % en comparación con el año anterior, según Arctic Wolf. A partir del cuarto trimestre de 2023, el pago promedio de rescate es de 568 705 dólares por víctima.

Es importante destacar que pagar un rescate no garantiza protección futura. No hay garantía de que los datos y sistemas de la víctima se recuperen de manera segura, ni de que los atacantes no vendan los datos robados en foros clandestinos o ataquen nuevamente.

Los datos compartidos por la empresa de ciberseguridad Cybereason revelan que "un sorprendente 78 % [de las organizaciones] fueron atacadas nuevamente después de pagar el rescate, el 82 % de ellas en un año", en algunos casos por el mismo actor de amenazas. Además, el 63 % de estas víctimas "se les solicitó pagar más la segunda vez".

The Hacker News. (s. f.-a). Phobos ransomware aggressively targeting U.S. critical infrastructure. https://thehackernews.com/2024/03/phobos-ransomware-aggressively.html

The Hacker News. (s. f.-c). VMware Issues Security Patches for ESXi, Workstation, and Fusion Flaws. https://thehackernews.com/2024/03/vmware-issues-security-patches-for-esxi.html

VMWARE PUBLICA PARCHES DE SEGURIDAD PARA FALLAS DE ESXI, ESTACIONES DE TRABAJO Y FUSION.

VMWARE HA LANZADO PARCHES PARA ABORDAR CUATRO VULNERABILIDADES DE SEGURIDAD QUE AFECTAN A ESXI, WORKSTATION Y FUSION, INCLUYENDO DOS FALLAS CRÍTICAS QUE PODRÍAN RESULTAR EN LA EJECUCIÓN DE CÓDIGO.

Identificadas como CVE-2024-22252 y CVE-2024-22253, estas vulnerabilidades se han clasificado como errores de uso después de la liberación en el controlador USB XHCI. Tienen una puntuación CVSS de 9.3 para Workstation y Fusion, y de 8.4 para sistemas ESXi.

"Un actor malintencionado con privilegios administrativos locales en una máquina virtual puede aprovechar este problema para ejecutar código como el proceso VMX de la máquina virtual que se ejecuta en el host", informó la compañía en un nuevo aviso.

"En ESXi, la explotación está contenida dentro del entorno limitado de VMX, mientras que, en Workstation y Fusion, esto puede llevar a la ejecución de código en la máquina donde está instalado Workstation o Fusion".

Varios investigadores de seguridad asociados con Ant Group Light-Year Security Lab y QiAnXin son reconocidos por descubrir e informar de forma independiente sobre CVE-2024-22252. Los investigadores de seguridad VictorV y Wei han sido reconocidos por informar sobre CVE-2024-22253.

El proveedor de servicios de virtualización propiedad de Broadcom también ha abordado otras dos vulnerabilidades:

- CVE-2024-22254 (puntuación CVSS: 7.9): una vulnerabilidad de escritura fuera de límites en ESXi que un actor malintencionado con privilegios dentro del proceso VMX podría aprovechar para desencadenar una fuga de la sandbox.
- CVE-2024-22255 (puntuación CVSS: 7.1): una vulnerabilidad de divulgación de información en el controlador USB UHCI que un atacante con acceso administrativo a una máquina virtual puede aprovechar para filtrar memoria del proceso vmx.

Estos problemas se han solucionado en las siguientes versiones, incluidas aquellas que han alcanzado el final de su vida útil (EoL) debido a la gravedad de estos problemas:

- ESXi 6.5 - 6.5U3v
- ESXi 6.7 - 6.7U3u
- ESXi 7.0 - ESXi70U3p-23307199
- ESXi 8.0: ESXi80U2sb-23305545 y ESXi80U1d-23299997
- VMware Cloud Foundation (VCF) 3.x
- Estación de trabajo 17.x - 17.5.1
- Fusión 13.x (macOS) - 13.5.1

Como solución temporal hasta que se pueda implementar un parche, se ha pedido a los clientes que eliminen todos los controladores USB de la máquina virtual.

CISA ADVIERTE: PIRATAS INFORMÁTICOS ATACAN ACTIVAMENTE LA VULNERABILIDAD DE MICROSOFT SHAREPOINT.

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha incluido una vulnerabilidad que afecta a Microsoft SharePoint Server en su catálogo de vulnerabilidades explotadas conocidas (KEV) basándose en pruebas de explotación activa en la naturaleza.

La vulnerabilidad, identificada como CVE-2023-24955 (con una puntuación CVSS de 7.2), es una grave falla de ejecución remota de código que permite a un atacante autenticado con privilegios de propietario del sitio ejecutar código arbitrario.

"En un ataque basado en red, un atacante autenticado como propietario del sitio podría ejecutar código de forma remota en el servidor SharePoint", afirmó Microsoft en un aviso. Esta falla fue corregida como parte de las actualizaciones del martes de parches de mayo de 2023.

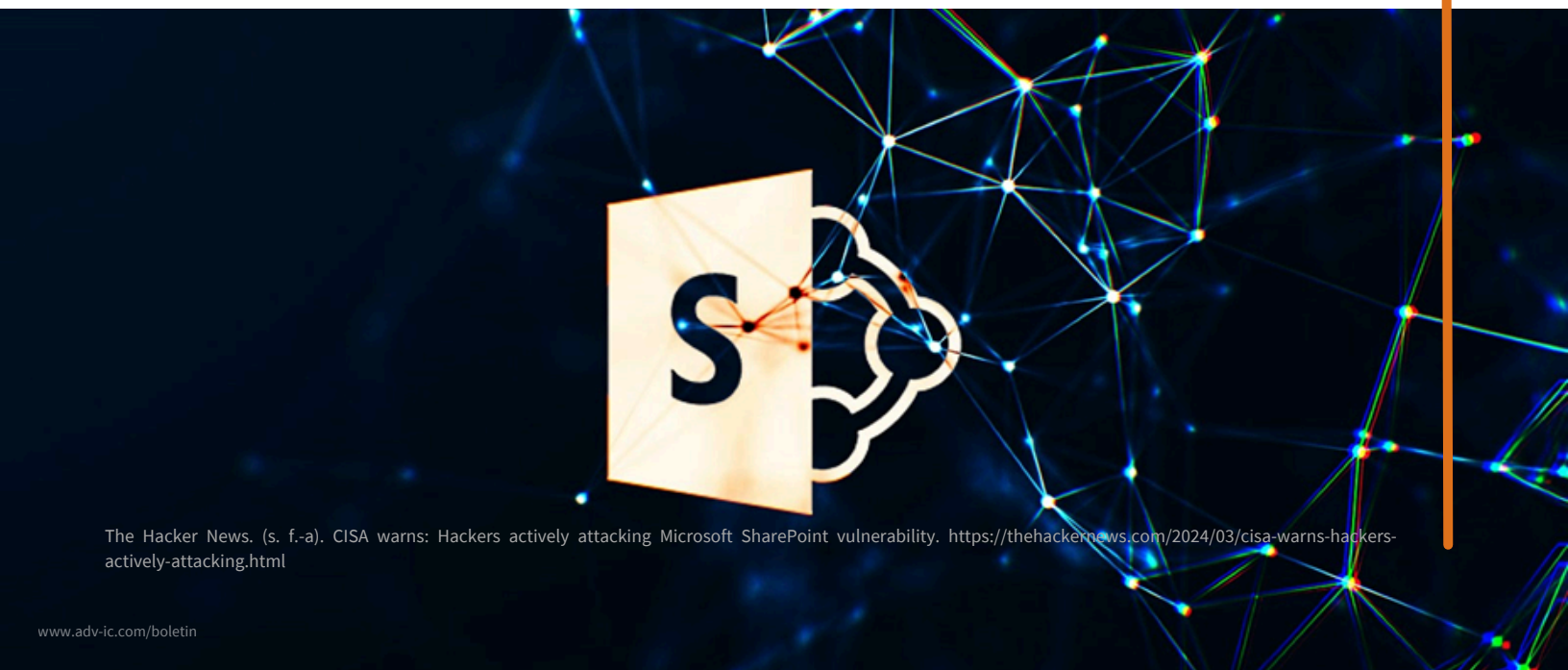
El desarrollo se produce más de dos meses después de que CISA agregara CVE-2023-29357, una falla de escalada de privilegios en SharePoint Server, a su catálogo KEV.

Es importante destacar que StarLabs SG demostró una cadena de exploits que combina CVE-2023-29357 y CVE-2023-24955 en el concurso de piratería Pwn2Own Vancouver el año pasado, lo que les valió a los investigadores un premio de 100.000 dólares.

Sin embargo, actualmente no hay información sobre los ataques que utilizan estas dos vulnerabilidades como armas ni sobre los actores de amenazas que podrían estar explotándolas.

Microsoft había informado previamente a The Hacker News que "los clientes que han habilitado las actualizaciones automáticas y habilitan la opción 'Recibir actualizaciones para otros productos de Microsoft' dentro de su configuración de Windows Update ya están protegidos".

Las agencias del Poder Ejecutivo Civil Federal (FCEB) deben aplicar las correcciones antes del 16 de abril de 2024 para proteger sus redes contra esta amenaza activa.



The Hacker News. (s. f.-a). CISA warns: Hackers actively attacking Microsoft SharePoint vulnerability. https://thehackernews.com/2024/03/cisa-warns-hackers-actively-attacking.html

EL NUEVO ATAQUE ZENHAMMER EVITA LAS DEFENSAS ROWHAMMER EN LAS CPU AMD.

Investigadores de ciberseguridad de ETH Zurich han desarrollado una nueva variante del ataque RowHammer contra la memoria DRAM (memoria dinámica de acceso aleatorio) que funciona con éxito en sistemas AMD Zen 2 y Zen 3, a pesar de las mitigaciones como Target Row Refresh (TRR).

Denominada ZenHammer, esta técnica representa la primera vez que se ha logrado explotar con éxito RowHammer en sistemas AMD, lo que amplía significativamente la superficie de ataque, considerando la cuota de mercado actual de AMD de alrededor del 36% en CPU de escritorio x86, según lo indicado por los investigadores.

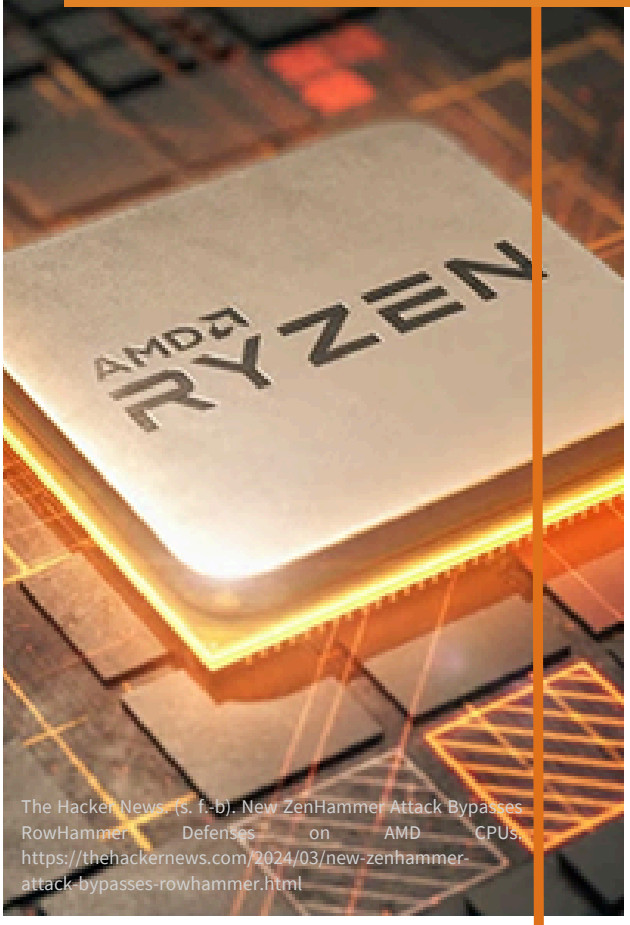
Además, ZenHammer también puede activar cambios de bits RowHammer en dispositivos DDR5 por primera vez.

RowHammer, que fue divulgado públicamente por primera vez en 2014, es un ataque bien conocido que aprovecha la arquitectura de celda de memoria DRAM para alterar datos. Este ataque consiste en acceder repetidamente a una fila específica de memoria (también conocido como "martilleo"), lo que provoca que la carga eléctrica de una celda se filtre a celdas adyacentes.

Esto puede inducir cambios aleatorios de bits en filas de memoria vecinas (de 0 a 1 o viceversa), lo que puede alterar el contenido de la memoria y potencialmente facilitar la escalada de privilegios, comprometiendo la confidencialidad, integridad y disponibilidad del sistema.

Vale la pena señalar que los módulos DRAM DDR5 se consideraban anteriormente inmunes a los ataques RowHammer debido a que reemplazaron TRR con un nuevo tipo de protección llamada administración de actualización.

INVESTIGADORES DE CIBERSEGURIDAD DE ETH ZURICH HAN DESARROLLADO UNA NUEVA VARIANTE DEL ATAQUE ROWHAMMER CONTRA LA MEMORIA DRAM



The Hacker News. (s. f.-b). New ZenHammer Attack Bypasses RowHammer Defenses on AMD CPUs. https://thehackernews.com/2024/03/new-zenhammer-attack-bypasses-rowhammer.html

"Los cambios en DDR5, como las mejoras en las mitigaciones de RowHammer, el código de corrección de errores (ECC) integrado y una frecuencia de actualización más alta (32 ms), hacen que sea más difícil activar el cambio de bits", explicaron los investigadores.

"A pesar de estos cambios, se necesita más investigación para comprender mejor las posibles nuevas mitigaciones de RowHammer y sus implicaciones para la seguridad, especialmente dado que se observaron cambios de bits en solo uno de cada diez dispositivos DDR5".

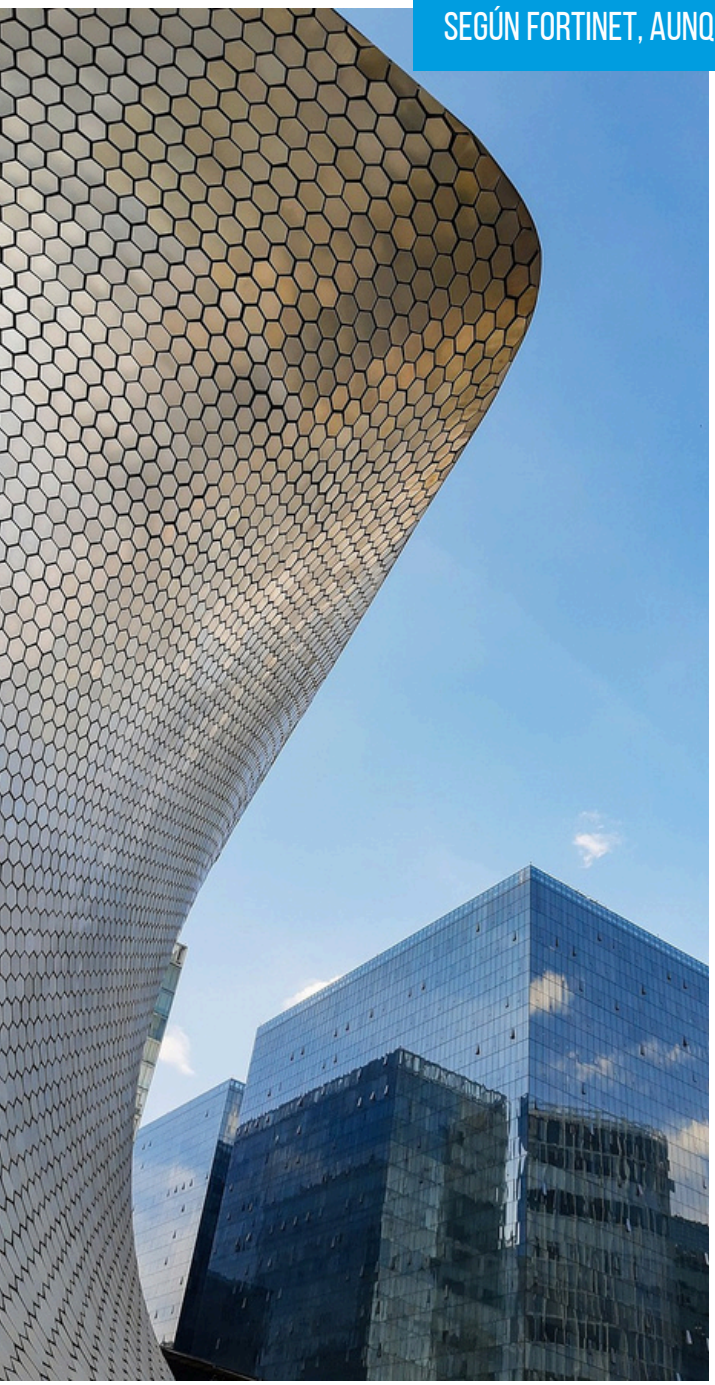
AMD, en un boletín de seguridad, declaró que está evaluando los cambios de bits de RowHammer en dispositivos DDR5 y que proporcionará una actualización una vez finalizado el proceso.

"Los productos de microprocesadores AMD incluyen controladores de memoria diseñados para cumplir con las especificaciones DDR estándar de la industria", añadió. "La susceptibilidad a los ataques RowHammer varía según el dispositivo DRAM, el proveedor, la tecnología y la configuración del sistema".

NOTICIAS NACIONALES

MÉXICO REGISTRÓ 94 MIL MILLONES DE INTENTOS DE CIBERATAQUES EN 2023, REVELA INFORME.

SEGÚN FORTINET, AUNQUE LA CIFRA REPRESENTA UNA DISMINUCIÓN CON RESPECTO AL 2022



Según Fortinet, aunque la cifra representa una disminución con respecto al 2022, los expertos advierten que esta tendencia no implica necesariamente una mejora en la seguridad cibernética.

México registró un total de 94 mil millones de intentos de ciberataques en 2023, según el laboratorio de análisis e inteligencia de amenazas de Fortinet.

Aunque esta cifra representa una disminución significativa con respecto a los 187 mil millones de intentos registrados en 2022, los expertos advierten que esta tendencia no necesariamente refleja una mejora en la seguridad cibernética.

Fortinet señaló que a nivel global se ha observado una disminución en la cantidad de ataques masivos, con un aumento en la sofisticación y enfoque de los ataques individuales. Esta tendencia se refleja en la menor cantidad de intentos de ciberataques en México, los cuales ahora están diseñados para objetivos específicos y son más difíciles de detectar y mitigar para las organizaciones que no cuentan con defensas de ciberseguridad integradas, automatizadas y actualizadas.

El reporte de la empresa de seguridad resalta que en la región de América Latina y el Caribe se registraron un total de 200 mil millones de intentos de ciberataques en 2023, representando el 14.5% del total global de ataques reportados el año pasado. Los países latinoamericanos más afectados fueron México, Brasil y Colombia.

En México, durante el cuarto trimestre de 2023, se observó un alarmante aumento exponencial en las actividades maliciosas detectadas, experimentando un crecimiento del 950% en comparación con el año anterior. Este incremento destaca la creciente sofisticación y agresividad de los ciberataques en el país, subrayando la urgencia de reforzar las medidas de ciberseguridad en las organizaciones.

MÉXICO REGISTRÓ 94 MIL MILLONES DE INTENTOS DE CIBERATAQUES EN 2023, REVELA INFORME.

Por otro lado, el ransomware continuó siendo una amenaza persistente en el panorama de ciberseguridad mexicano, con ataques que se vuelven cada vez más específicos y dirigidos.

Durante 2023, se observó una presencia significativa de amenazas vinculadas a aplicaciones de Microsoft Office, como Excel, Word y PowerPoint, las cuales representaron casi el 50% de todas las detecciones de malware en México.

En cuanto al malware Prometei, que tiene la capacidad de controlar de forma remota las máquinas infectadas, se detectó un aumento de actividad en Latinoamérica durante el 2023. Países como Panamá y Ecuador fueron especialmente afectados, lo que subraya la importancia de implementar medidas de protección adicionales para mitigar los riesgos asociados con este tipo de amenazas.

Por otro lado, la explotación Double Pulsar fue identificada como la vulnerabilidad predominante en casi todos los países de Latinoamérica, representando el 75% de toda la actividad maliciosa detectada en el último trimestre de 2023.

Hernández, A. (2024, 25 marzo). México [illegible] mil millones de intentos de ciberataques en 2023, revela informe. El Universal. https://www.eluniversal.com.mx/cartera/mexico-registro-94-mil-millones-de-intentos-de-ciberataques-en-2023-revela-informe/

MÉXICO REGISTRA BRECHAS DE CIBERSEGURIDAD POR MÁS DE 7 MIL MILLONES DE PESOS.

Los estudios e informes sobre el panorama de la ciberseguridad en México son contundentes. Según un estudio de IDC realizado en 2023, el costo promedio de una brecha de seguridad en México fue de 7.2 millones de pesos.

Por otro lado, una encuesta de EY realizada en 2022 encontró que el 70% de las empresas mexicanas habían experimentado un ataque cibernético en el último año. Además, el reporte de la Asociación Mexicana de Instituciones de Seguros (AMIS) sobre delitos cibernéticos en 2023 indicó que se recibieron 110,000 denuncias por este tipo de delitos, con un monto total de 7,345 millones de pesos en pérdidas.

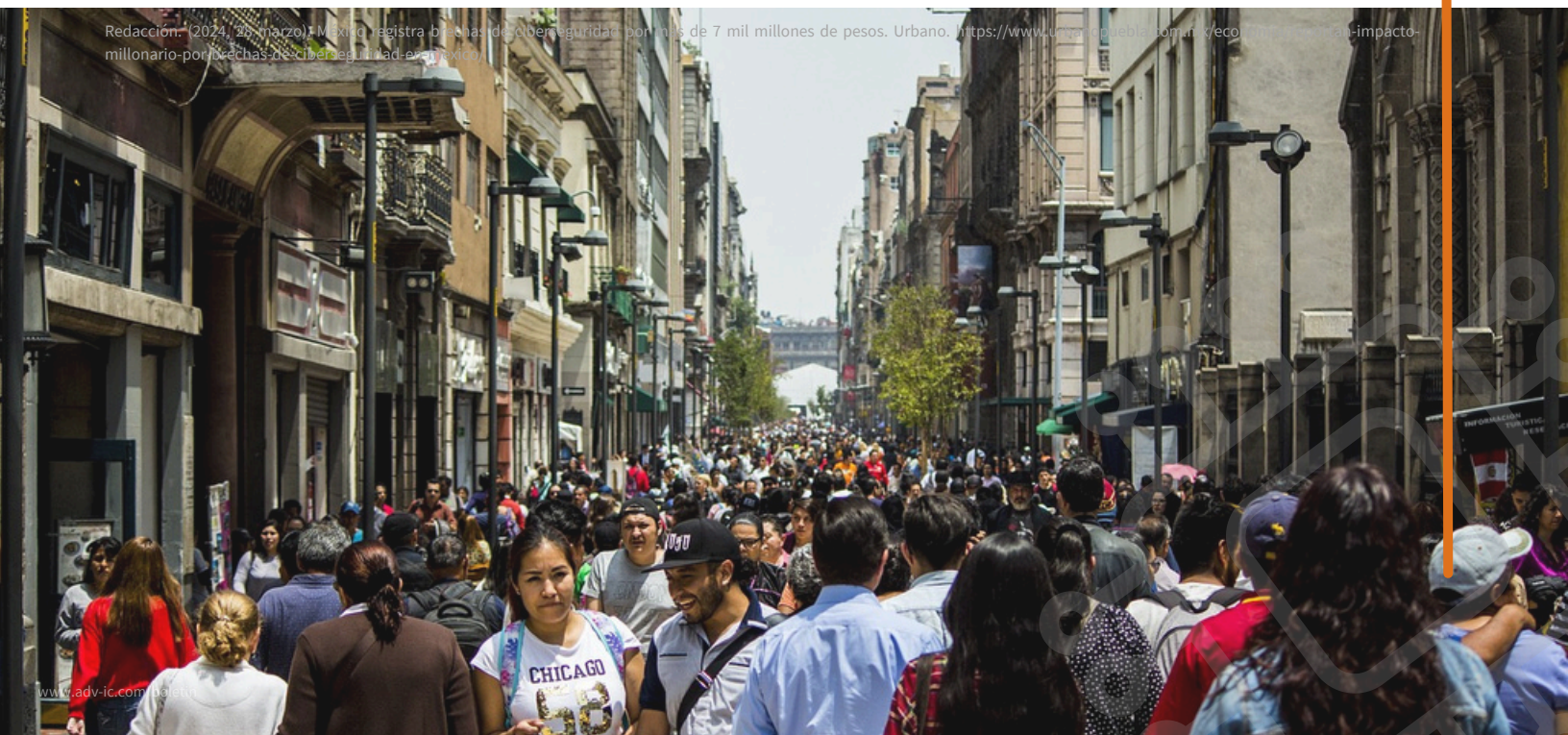
En este contexto, ETEK, proveedor líder de servicios gestionados de ciberseguridad, anuncia la llegada a México de Cyble, la plataforma de inteligencia de amenazas más innovadora del mundo.

Esta alianza estratégica tiene como objetivo fortalecer la ciberseguridad de las empresas mexicanas ante el panorama cada vez más complejo y desafiante de las amenazas digitales.

La alianza entre ETEK y Cyble representa un hito en la evolución de la ciberseguridad en México. Ambas compañías unen su experiencia y conocimiento para ofrecer a las empresas mexicanas una solución integral y proactiva que les permita:

- Reducir el riesgo de sufrir un ataque cibernético.
- Detectar las amenazas de forma temprana y precisa.
- Responder a los incidentes de manera rápida y efectiva.
- Minimizar el impacto de las brechas de seguridad.

La inteligencia de amenazas se ha convertido en un elemento fundamental en las estrategias de ciberseguridad y ciberdefensa. La plataforma de Cyble ofrece una visión completa del panorama de amenazas, permitiendo a las empresas anticiparse a los riesgos y tomar medidas proactivas para protegerse. Con esta alianza, las empresas mexicanas pueden aprovechar esta inteligencia de amenazas para fortalecer su postura de seguridad cibernética y mitigar los riesgos asociados con las crecientes amenazas cibernéticas.



Redacción. (2024, 26 marzo). México registra brechas de ciberseguridad por más de 7 mil millones de pesos. Urbano. https://www.urbanopuebla.com.mx/economia/mexico-impacto-millonario-por-brechas-de-ciberseguridad-en-mexico/

Arenas, J. (2024, 15 marzo). México y España firman un acuerdo para fortalecer la ciberseguridad en las TIC. Segurilatam. https://www.segurilatam.com/ciberilatam/mexico-y-espana-firman-un-acuerdo-para-fortalecer-la-ciberseguridad-en-las-tic_20240315.html

MÉXICO Y ESPAÑA FIRMAN UN ACUERDO PARA FORTALECER LA CIBERSEGURIDAD EN LAS TIC.

El Instituto Federal de Telecomunicaciones de México y el Instituto Nacional de Ciberseguridad de España (Incibe) han firmado un acuerdo de colaboración para potenciar la ciberseguridad en varias áreas. El objetivo es promover el desarrollo seguro y sostenible de las tecnologías de la información y la comunicación (TIC) en ambos países.

Este convenio, con una duración inicial de tres años y posibilidad de prórroga, se centra en la colaboración para desarrollar una conciencia en seguridad cibernética fuerte y resiliente, así como abordar los desafíos del actual contexto digital.

Entre las iniciativas que se llevarán a cabo como parte de este acuerdo se encuentran la organización de eventos dirigidos a usuarios de telecomunicaciones, la implementación de normas y reglamentos técnicos, la realización de análisis y evaluaciones sobre vulnerabilidades, y la mejora de las capacidades en laboratorios para homologar productos destinados a las telecomunicaciones.

En resumen, este acuerdo busca fortalecer la colaboración entre México y España en materia de ciberseguridad, con el objetivo de proteger y promover el desarrollo seguro de las TIC en ambos países.

MÉXICO: UN BLANCO VULNERABLE EN EL PANORAMA GLOBAL DE LA CIBERSEGURIDAD.

La importancia de implementar la ciberseguridad en los procesos empresariales es fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información en un mundo cada vez más interconectado. La protección de datos sensibles y la salvaguardia de la infraestructura crítica, como los sistemas financieros, de salud y energía, son elementos clave en la lucha contra las amenazas cibernéticas maliciosas.

En el ciberespacio, México enfrenta un panorama desafiante, con un promedio de 1,607 ciberataques semanales desde 2023. Según un informe anual de ciberataques del 2024, México ocupa el sexto lugar en el total de ataques de ransomware a nivel mundial. Se ha observado un aumento significativo en el volumen mundial de ataques criptográficos, así como un aumento en las amenazas cifradas, ya que los ciberdelincuentes optan por medios más sigilosos y menos arriesgados para sus actividades maliciosas.

Frente a estos desafíos, compañías como ITAC continúan desarrollando software de seguridad y protección de datos que aborda las necesidades y desafíos principales de las empresas. Esto incluye la sofisticación creciente de las amenazas cibernéticas, el cumplimiento de regulaciones de seguridad cada vez más estrictas y la protección de datos sensibles en entornos de nube híbrida y B2B.

El desarrollo de software de seguridad integrado con inteligencia artificial (IA) es fundamental en México debido al aumento de las amenazas cibernéticas y la creciente dependencia de la tecnología en todas las industrias. La IA puede mejorar la capacidad de detección y respuesta de las organizaciones a los ataques cibernéticos al analizar grandes volúmenes de datos en tiempo real e identificar patrones y anomalías que podrían indicar actividad maliciosa.

Héctor Triana, Director Comercial de ITAC, comenta que este proceso se lleva a cabo de manera progresiva, cuidadosa y meticulosa, asegurándose de implementar medidas sólidas de protección de datos para garantizar la confidencialidad de la información de los clientes en todo momento.

Villaseñor, C. (2024, 27 marzo). México: Un blanco vulnerable en el panorama global de la ciberseguridad. CIO | EOMWORLD. https://iworld.com.mx/mexico-un-blanco-vulnerable-en-el-panorama-global-de-la-ciberseguridad-2/

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: MARZO 2024

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-48788	12/03/2024	Fallas de seguridad en productos Fortinet	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2023-48788

Descripción: Una neutralización inadecuada de elementos especiales utilizados en un comando sql ("inyección sql") en Fortinet FortiClientEMS versión 7.2.0 a 7.2.2, FortiClientEMS 7.0.1 a 7.0.10 permite a un atacante ejecutar código o comandos no autorizados a través de paquetes especialmente diseñados.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-21400	12/03/2024	Fallas de seguridad en productos Microsoft Azure	CVSS v3.1: 9.0 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2024-21400

Descripción: Vulnerabilidad de elevación de privilegios del contenedor confidencial del servicio Microsoft Azure Kubernetes.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-42789	12/03/2024	Fallas de seguridad en productos Fortinet	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2023-42789

Descripción: Una escritura fuera de límites en Fortinet FortiOS 7.4.0 a 7.4.1, 7.2.0 a 7.2.5, 7.0.0 a 7.0.12, 6.4.0 a 6.4.14, 6.2.0 a 6.2.15, FortiProxy 7.4.0, 7.2.0 a 7.2.6, 7.0.0 a 7.0.12, 2.0.0 a 2.0.13 permite a un atacante ejecutar código o comandos no autorizados a través de solicitudes HTTP especialmente diseñadas.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-36554	12/03/2024	Fallas de seguridad en productos Fortinet	CVSS v3.1: 9.8 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2023-36554

Descripción: Un control de acceso inadecuado en Fortinet FortiManager versión 7.4.0, versión 7.2.0 a 7.2.3, versión 7.0.0 a 7.0.10, versión 6.4.0 a 6.4.13, 6.2 todas las versiones permiten a un atacante ejecutar código o comandos no autorizados a través de solicitudes HTTP especialmente diseñadas.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-28578	04/03/2024	Fallas de seguridad en productos Qualcom	CVSS v3.1: 9.3 [critico]	https://nvd.nist.gov/vuln/detail/CVE-2023-28578

Descripción: Corrupción de la memoria en los servicios principales al ejecutar el comando para eliminar un único detector de eventos.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-27266	14/03/2024	Fallas de seguridad en productos IBM	CVSS v3.1: 8.2 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2024-27266

Descripción: IBM Maximo Application Suite 7.6.1.3 es vulnerable a un ataque de inyección de entidad externa XML (XXE) al procesar datos XML. Un atacante remoto podría aprovechar esta vulnerabilidad para exponer información confidencial o consumir recursos de memoria. ID de IBM X-Force: 284566.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-26204	12/03/2024	Fallas de seguridad en productos Microsoft	CVSS v3.1: 7.5 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2024-23477

Descripción: Vulnerabilidad de divulgación de información de Outlook para Android

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-26199	12/03/2024	Fallas de seguridad en productos Microsoft	CVSS v3.1: 7.8 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2024-26199

Descripción: Vulnerabilidad de elevación de privilegios de Microsoft Office

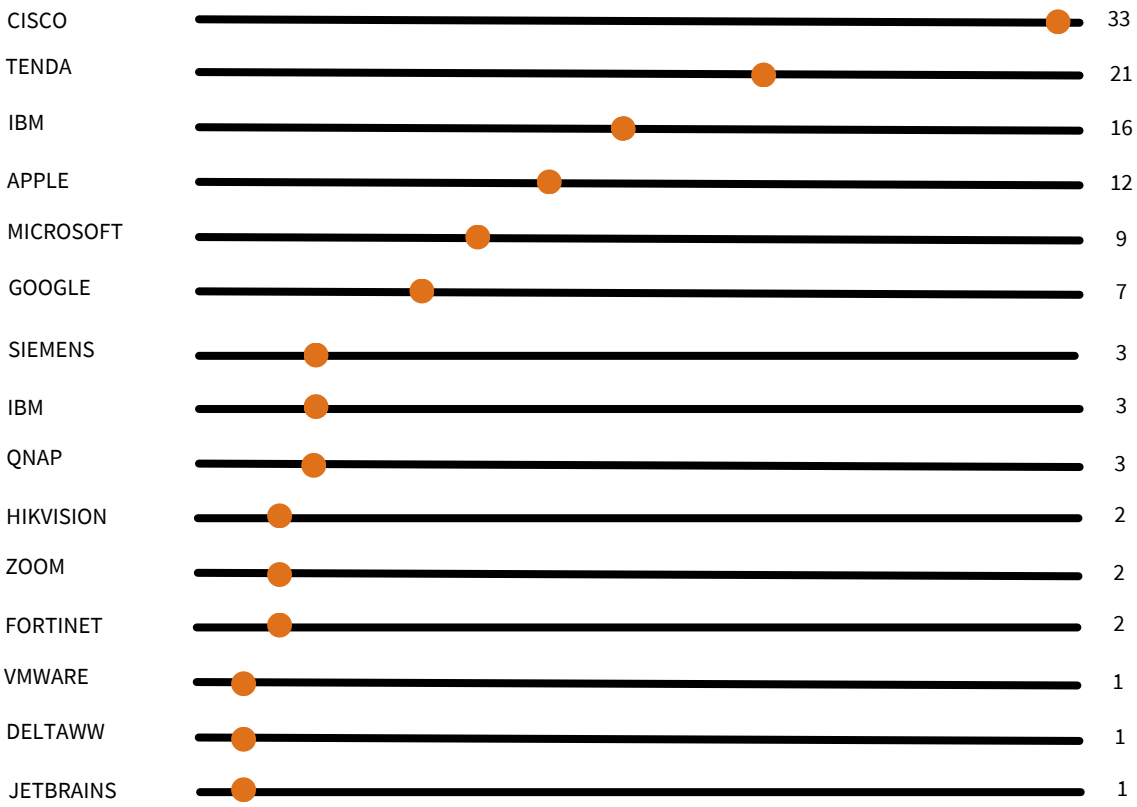
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-42790	12/03/2024	Fallas de seguridad en productos Fortinet	CVSS v3.1: 8.1 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2023-42790

Descripción: Esta vulnerabilidad ha sido modificada desde la última vez que fue analizada por el NVD. Está a la espera de un nuevo análisis que puede dar lugar a nuevos cambios en la información proporcionada.

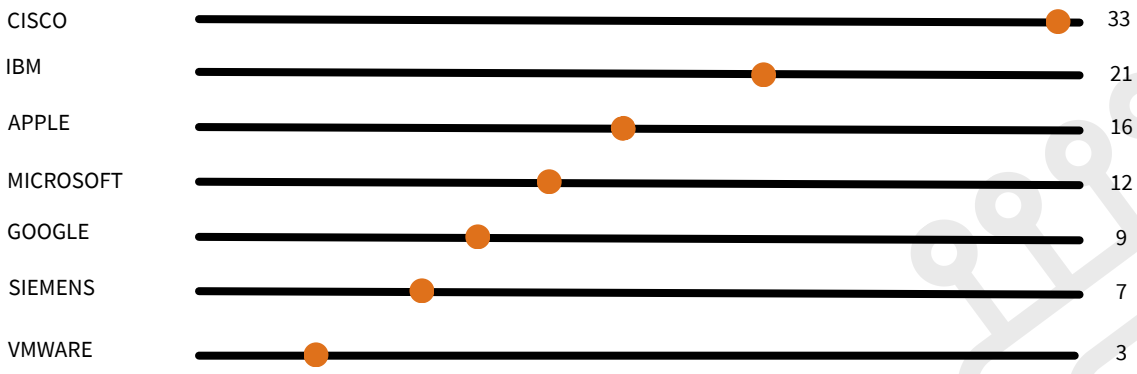
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2024-21445	12/03/2024	Fallas de seguridad en productos Microsoft	CVSS v3.1: 7.0 [Alto]	https://nvd.nist.gov/vuln/detail/CVE-2024-21445

Descripción: Vulnerabilidad de elevación de privilegios del controlador de impresión USB de Windows

FABRICANTES CON VULNERABILIDADES RELEVANTES: MARZO DE 2024



EMPRESAS MULTINACIONALES CON VULNERABILIDADES: MARZO DE 2024



CULTURA DE CIBERSEGURIDAD

MEDIOS EXTRAÍBLES

PRECAUCIÓN

Si encuentras una memoria USB u otro dispositivo de almacenamiento portátil en el entorno “natural”, es imperativo no conectarlo a tu computadora. ¿Por qué? Pues bien, nunca se debe conectar una unidad extraíble a menos que se conozca y confíe en su origen, o si se toman medidas especiales para garantizar que no pueda dañar el dispositivo. Imagina que te topas con un dongle USB, una unidad flash o cualquier otro dispositivo similar. Es posible que te sientas tentado a conectarlo para averiguar quién es su propietario o, incluso, por la posibilidad de obtener algo gratuito.

Sin embargo, utilizar medios extraíbles encontrados te expone a riesgos significativos. Deberías considerar esta situación de la misma manera que aseguras tu casa: mediante medidas básicas de seguridad, como el uso de contraseñas robustas y otras prácticas recomendadas en ciberseguridad. Conectar una unidad extraña equivale a entregar las llaves de tu casa virtual a un desconocido, lo que podría permitirle acceder a tu sistema de forma no autorizada.

Eitel, B. (2023, 1 junio). Dongles, sticks, unidades y llaves: lo que hay que saber sobre los medios extraíbles. Alianza Nacional de Ciberseguridad. https://staysafeonline.org/es/online-safety-privacy-basics/best-practices-for-removable-media-and-devices/

¿QUE SON LOS MEDIOS EXTRAIBLES?

Los medios extraíbles, también conocidos como dispositivos de almacenamiento portátil, son hardware que se puede transportar fácilmente. Las unidades flash USB son muy comunes, pero también se incluyen discos duros externos utilizados para realizar copias de seguridad de computadoras, así como tarjetas SD que se encuentran en cámaras digitales.

A pesar de que muchas personas optan por realizar copias de seguridad de sus archivos en la nube, los medios extraíbles siguen siendo ampliamente utilizados. Además, están surgiendo nuevos usos, como el uso de unidades USB como billeteras portátiles para almacenar criptomonedas.

Es importante tener en cuenta que una unidad USB encontrada en un lugar inusual, como en el suelo de una oficina o en un área cubierta de hierba junto a un camino transitado, podría representar un riesgo. Aunque es posible que la unidad simplemente se haya extraviado, también existe la posibilidad de que haya sido colocada allí de manera intencional, especialmente si se encuentra en un entorno laboral. Incluso si el propietario original de la unidad no es un pirata informático, podría contener malware, virus u otras amenazas que podrían infectar tu dispositivo si lo conectas.

En resumen, es importante tener precaución al encontrar medios extraíbles, ya que podrían representar una amenaza para la seguridad de tu dispositivo y tu red. Es como considerar si comieses comida encontrada en el suelo o en una mesa al azar: es mejor proceder con cautela.

REFERENCIAS

REFERENCIAS

- The Hacker News. (s. f.). Urgent: Secret Backdoor Found in XZ Utils Library, Impacts Major Linux Distros. https://thehackernews.com/2024/03/urgent-secret-backdoor-found-in-xz.html
- The Hacker News. (s. f.-a). Phobos ransomware aggressively targeting U.S. critical infrastructure. https://thehackernews.com/2024/03/phobos-ransomware-aggressively.html
- The Hacker News. (s. f.-c). VMware Issues Security Patches for ESXi, Workstation, and Fusion Flaws. https://thehackernews.com/2024/03/vmware-issues-security-patches-for-esxi.html
- The Hacker News. (s. f.-a). CISA warns: Hackers actively attacking Microsoft SharePoint vulnerability. https://thehackernews.com/2024/03/cisa-warns-hackers-actively-attacking.html
- The Hacker News. (s. f.-b). New ZenHammer Attack Bypasses RowHammer Defenses on AMD CPUs. https://thehackernews.com/2024/03/new-zenhammer-attack-bypasses-rowhammer.html
- Hernández, A. (2024, 25 marzo). México registró 94 mil millones de intentos de ciberataques en 2023, revela informe. El Universal. https://www.eluniversal.com.mx/cartera/mexico-registro-94-mil-millones-de-intentos-de-ciberataques-en-2023-revela-informe/
- Redacción. (2024, 28 marzo). México registra brechas de ciberseguridad por más de 7 mil millones de pesos. Urbano. https://www.urbanopuebla.com.mx/economia/reportan-impacto-millonario-por-brechas-de-ciberseguridad-en-mexico/
- Arenas, J. (2024, 15 marzo). México y España firman un acuerdo para fortalecer la ciberseguridad en las TIC. Segurilatam. https://www.segurilatam.com/ciberilatam/mexico-y-espana-firman-un-acuerdo-para-fortalecer-la-ciberseguridad-en-las-tic_20240315.html
- Villaseñor, C. (2024, 27 marzo). México: Un blanco vulnerable en el panorama global de la ciberseguridad. CIO | EDIWORLD. https://iworld.com.mx/mexico-un-blanco-vulnerable-en-el-panorama-global-de-la-ciberseguridad-2/
- Eitel, B. (2023, 1 junio). Dongles, sticks, unidades y llaves: lo que hay que saber sobre los medios extraíbles. Alianza Nacional de Ciberseguridad. https://staysafeonline.org/es/online-safety-privacy-basics/best-practices-for-removable-media-and-devices/

ZERU Cybersecurity Services

Security Operation Center - SOC by

+52 81 2011 8604

contacto@adv-ic.com

Av. Melchor Ocampo 193, Torre Privanza, Piso 11 Oficina 11D
Colonia Veronica Anzures. Delegación Miguel Hidalgo CP 11300

Visita nuestra página Web