



¿Están las
organizaciones
atravesando una
crisis de identidad?

2024

Informe de Vulnerabilidades de Microsoft



Beneficiarse de conocimientos
respaldados por investigaciones y
análisis de expertos de la industria
para proteger mejor su patrimonio de
Microsoft en 2024 y más allá



TABLA DE CONTENIDO

Resumen ejecutivo	2
Hallazgos clave y datos destacados	3
Vulnerabilidades destacadas	17
¿Están las organizaciones atravesando una crisis de identidad?	24
¿Qué dicen los expertos?	28
Mitigando los riesgos del ecosistema Microsoft para mejorar la resiliencia cibernética	38
Cómo BeyondTrust mitiga las vulnerabilidades tradicionales y los riesgos modernos basados en identidades	39
Conclusión	40
Metodología	41
Recursos adicionales	42



Resumen Ejecutivo

La 11ª edición del Informe de Vulnerabilidades de Microsoft trae una pregunta clave mientras analizamos el panorama de las vulnerabilidades:

"¿Están las organizaciones atravesando una crisis de identidad?"



A lo largo de sus 11 años de publicación, el Informe de vulnerabilidades de Microsoft ha obtenido más de 16 000 descargas y ha ayudado a miles de usuarios a aprovechar su análisis de datos detallado y los hallazgos de expertos para mejorar sus defensas cibernéticas.

La edición de este año no solo analiza los datos de vulnerabilidades de Microsoft de 2023, sino que también evalúa cómo se aprovechan estas vulnerabilidades en ataques basados en identidades. El informe también destaca algunos de los CVEs más importantes de 2023 (puntuación de gravedad CVSS > 9.0), desglosa cómo los aprovechan los atacantes y explica cómo pueden mitigarse.

Algunos de los principales expertos en ciberseguridad del mundo comparten sus opiniones sobre los hallazgos del informe mientras fijamos colectivamente nuestra mirada en las amenazas emergentes, las nuevas vulnerabilidades y la mejor manera de desarrollar la resiliencia cibernética en toda la empresa y la sociedad en general.

Siga leyendo para comprender, identificar y abordar mejor los riesgos que enfrenta su organización dentro del ecosistema Microsoft.

Hallazgos Clave y Datos Destacados

Hallazgos Clave

Después de alcanzar un máximo histórico en el número de vulnerabilidades reportadas en 2022, el total de vulnerabilidades reportadas ha disminuido ligeramente.

Si analizamos la tendencia más amplia, el número de vulnerabilidades se ha estancado desde 2020.

El total de vulnerabilidades continúa cerca de sus cifras más altas jamás registradas. Si bien disminuyeron ligeramente (un 5%) de 1292 a 1228 en 2023, el total de vulnerabilidades se mantuvo firme cerca de sus máximos históricos, permaneciendo entre 1200 y 1300 durante los últimos cuatro años (desde 2020).

Elevación de Privilegios sigue siendo la categoría dominante. Continuando la tendencia en los años posteriores a la pandemia, la elevación de privilegios representó el 40% (490) del total de vulnerabilidades en 2023.

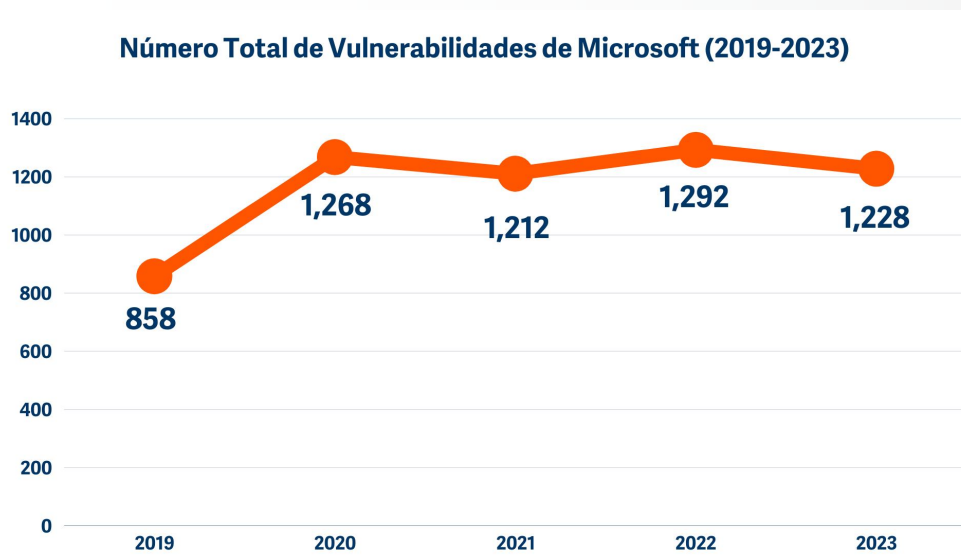
El número total de vulnerabilidades críticas continúa su tendencia a la baja, pero lentamente. Las vulnerabilidades críticas se redujeron un 6% a 84 en 2023 (5 menos que en 2022).



Datos Destacados

- Después de que las vulnerabilidades de Microsoft Azure y Dynamics 365 se dispararan en 2022, se redujeron casi a la mitad en 2023: de 114 a 63.
- Microsoft Edge experimentó 249 vulnerabilidades en 2023, de las cuales solo una fue crítica.
- Hubo 522 vulnerabilidades de Windows en 2023, 55 de las cuales fueron críticas.
- Microsoft Office experimentó 62 vulnerabilidades en 2023.
- La categoría Windows Server tuvo 558 vulnerabilidades en 2023, 57 de las cuales fueron críticas.
- Las vulnerabilidades de denegación de servicio aumentaron un 51% hasta alcanzar un nivel récord de 109 en 2023, y la suplantación de identidad demostró un espectacular aumento del 190 %, de 31 a 90 .

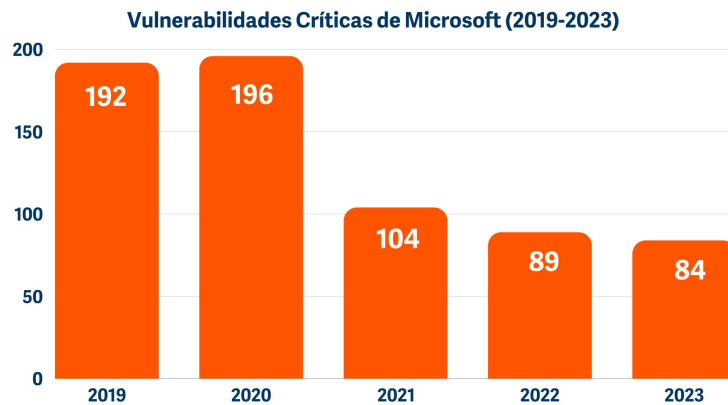
Tendencia de 5 años



El número total de vulnerabilidades se ha estancado y se mantiene entre 1200 y 1300 durante los últimos cuatro años.

Tras el dramático aumento de las vulnerabilidades de Microsoft en 2020, hemos observado que el número se estancó en los últimos cuatro años, con el rango de fluctuaciones manteniéndose dentro de una ventana del 7%.

El número total alcanzó 1228 en 2023, lo que representa una disminución del 5% con respecto al año anterior, después de alcanzar un máximo histórico de 1292 en 2022.

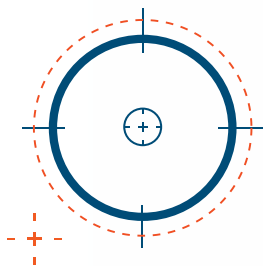


Las **vulnerabilidades críticas** continuaron su tendencia a la baja en 2023, pero el ritmo se ha desacelerado.

De manera similar, las vulnerabilidades críticas se han mantenido estables, disminuyendo ligeramente de 89 en 2022 a 84 en 2023. En términos de vulnerabilidades totales y críticas, esto hace que los últimos dos años sean algunos de los más consistentes que hemos visto desde el debut de este informe hace once años, sin cambios importantes en los datos principales.

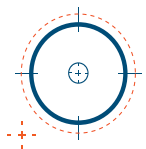
Al observar la distribución de vulnerabilidades críticas año tras año, observamos una tendencia a la baja constante. Las categorías Windows Desktop y Server han seguido siendo la principal fuente de vulnerabilidades críticas hasta 2023. Dado que comparten una base de código similar, lo que representa una evolución progresiva del kernel de Windows NT, esto no es una sorpresa.

Como comentamos en el informe del año pasado, hay áreas de sistemas operativos Windows con códigos de hace aproximadamente 20 años, a menudo olvidados hace mucho tiempo, que pueden volver en nuestra contra, incluso en las últimas versiones de Windows. Con el tiempo, estos riesgos han ido disminuyendo constantemente a medida que se ha actualizado la larga lista de servicios y funciones. Esto juega un papel en el motivo por el cual estamos viendo estabilidad en los datos hoy, lo cual cubriremos con mayor profundidad a continuación.



Las vulnerabilidades críticas - una importante fuente de riesgo para las organizaciones de todo el mundo - cuando se explotan, tienen el potencial de provocar eventos de seguridad de alto impacto. Estas son las vulnerabilidades que mantienen despiertos a los administradores de TI por la noche.

¿Qué nos dicen los datos de vulnerabilidades estables?



Los datos de vulnerabilidades estables son un fuerte indicador de que los esfuerzos generales de seguridad a largo plazo están dando sus frutos.

Como comentamos en informes anteriores, la ausencia de aumentos bruscos, así como una disminución constante de las cifras, son buenos indicadores de que muchos de los esfuerzos de seguridad a largo plazo de Microsoft están dando sus frutos.

Los productos heredados, muchos de los cuales se desarrollaron por primera vez antes de que Microsoft introdujera su ciclo de vida de desarrollo de seguridad en 2004, han llegado al final de su vida útil (EOL), y sistemas operativos y productos más nuevos y más seguros han tomado su lugar. Las tecnologías de la nube han madurado y esas inversiones en seguridad han dado sus frutos.

Incluso mirando hacia atrás tan solo tres años, vemos un panorama completamente diferente. En 2020, las cifras de vulnerabilidades críticas fueron un 133% más altas que en 2023. Si bien los datos de este año no han revelado una disminución tan grande en las vulnerabilidades críticas como en años anteriores, la constante tendencia a la baja continúa. Este es un hallazgo tranquilizador, especialmente para los profesionales de TI que viven y respiran la seguridad de sus sistemas Microsoft.

Entendiendo las Vulnerabilidades Críticas de Microsoft

El número total de vulnerabilidades es un indicador importante de la salud de un entorno, pero las vulnerabilidades no se crean de la misma manera.

Algunas pueden plantear riesgos principalmente teóricos (baja probabilidad y bajo impacto) si son explotadas. En el lado opuesto del espectro, otras tienen altas probabilidades de ser explotadas, y su explotación puede tener un impacto muy negativo para las organizaciones afectadas.

Medir el nivel de impacto de la vulnerabilidad se relaciona con su impacto en la confidencialidad, integridad y disponibilidad de los datos dentro de un sistema u organización. Las vulnerabilidades más graves afectarán estos tres principios básicos de seguridad de la información.

Las vulnerabilidades clasificadas como "críticas" son aquellas con características que hacen que su explotación sea potencialmente de alto impacto para la seguridad del evento. La forma en que Microsoft clasifica el índice de gravedad de una vulnerabilidad es distinta de la probabilidad de explotación.

Sin embargo, la probabilidad de explotación es mucho más dinámica porque es más probable que los atacantes aprovechen una vulnerabilidad conocida.

La explotación de vulnerabilidades "críticas":

Probablemente resulte en un compromiso total de un dispositivo o infraestructura.

Tendrá menos requisitos previos. Por lo general, el ataque no requeriría ningún acceso especial, privilegios o conocimientos avanzados.

Permitirá la ejecución de código sin interacción del usuario. Por lo general, no se basan en la ingeniería social.

Este tipo de vulnerabilidades es lo que mantienen despiertos a los administradores de TI por la noche y son una fuente importante de riesgo con la que deben lidiar las empresas de todo el mundo.



¿Cómo clasifica Microsoft las vulnerabilidades críticas?

El [National Vulnerabilities Database \(NVD\)](#) clasifica las vulnerabilidades críticas como aquellas a las que se les ha otorgado la puntuación de 9.0-10.0 según el [Sistema de puntuación de vulnerabilidad común \(CVSS\)](#). Los lectores más entusiastas de los anuncios de vulnerabilidades de Microsoft pueden haber notado que, si bien Microsoft ahora utiliza la puntuación CVSS 3.1 para sus vulnerabilidades, clasifica las gravedades basándose en el propio sistema de clasificación de seguridad. Esto clasifica cada vulnerabilidad de acuerdo con el peor resultado teórico en caso de que se explote esa vulnerabilidad.

Esto significa que:

Si bien 33 vulnerabilidades obtuvieron una puntuación de 9.0 o superior en 2023 (un aumento del 50% respecto de las 22 de 2022), y por lo tanto consideradas "críticas" según el sistema de puntuación, Microsoft ha clasificado 84 de sus vulnerabilidades como críticas en 2023 (un 6% menos que las 89 de 2022).

Clasificaciones CVSS 3.1

Severidad	Rango de puntuación base
Ninguna	0.0
Baja	0.1 - 3.9
Media	4.0 - 6.9
Alta	7.0 - 8.9
Crítica	9.0 - 10.0

Fig. 1: El sistema de puntuación de la Base de datos nacional de vulnerabilidades (NVD) para clasificar vulnerabilidades críticas

Sistema de Clasificación de Actualizaciones de Seguridad de Microsoft | Calificación y descripción

Crítica

Una vulnerabilidad cuya explotación podría permitir la ejecución de código sin interacción del usuario. Estos escenarios incluyen malware que se propaga automáticamente (p. ej. worms de red), o escenarios de uso común evitables donde la ejecución del código se produce sin advertencias ni indicaciones. Esto podría significar navegar a una página web o abrir un correo electrónico. Microsoft recomienda que los clientes apliquen actualizaciones críticas de inmediato.

Importante

Una vulnerabilidad cuya explotación podría comprometer la confidencialidad, integridad o disponibilidad de los datos del usuario, o de la integridad o disponibilidad de los recursos de procesamiento. Estos escenarios incluyen los de uso común en los que un cliente se ve comprometido con advertencias o avisos independientemente de la procedencia, calidad o usabilidad del aviso. También se tratan las secuencias de acciones del usuario que no generan avisos o advertencias. Microsoft recomienda que los clientes apliquen actualizaciones importantes lo antes posible.

Moderado

El impacto de la vulnerabilidad se mitiga en gran medida por factores como los requisitos de autenticación o la aplicabilidad sólo a configuraciones no predeterminadas. Microsoft recomienda que los clientes consideren aplicar la actualización de seguridad.

Bajo

El impacto de la vulnerabilidad se mitiga de manera integral mediante las características del componente afectado. Microsoft recomienda que los clientes evalúen si vale aplicar la actualización de seguridad a los sistemas afectados.

Fig 2: El Sistema de Clasificación de Gravedad de las Actualizaciones de Seguridad de Microsoft que identifica el riesgo asociado en función del peor resultado teórico, si esa vulnerabilidad fuera explotada.



Vale la pena señalar la diferencia entre la puntuación CVSS y el sistema de clasificación de gravedad de Microsoft, no solo al considerar los datos de este informe, sino también al considerar el riesgo en su organización.

El sistema CVSS considera la gravedad técnica de una vulnerabilidad (es decir, si una vulnerabilidad resulta en alguna pérdida de confidencialidad de los datos o en una pérdida total de confidencialidad). La puntuación CVSS no mide el riesgo de esa vulnerabilidad. Esto significa que las puntuaciones CVSS por sí solas no pueden indicarle si una vulnerabilidad causará un impacto de misión crítica en un sistema, o si la pérdida limitada de algunos datos altamente confidenciales tendría un impacto más severo que la pérdida total de datos no confidenciales.

El sistema de clasificación de gravedad de Microsoft es potencialmente mucho más útil que una puntuación CVSS base o temporal para los profesionales de la seguridad que intentan priorizar la reducción de riesgos. Sin embargo, es importante conocer su propio entorno y sus riesgos para que pueda comprender cuál es la mejor manera de priorizar los parches y/o utilizar otros controles y mitigaciones para reforzar la seguridad.

Todos los datos proporcionados por el sistema de clasificación de gravedad de Microsoft se basa en la información disponible en ese momento. Carece del contexto de los modelos de amenazas de su propia empresa. Lo que se considera un parche crítico para una organización puede no serlo para otra; todo depende del contexto empresarial.

Además de su [Sistema de clasificación de gravedad](#) de actualización de seguridad. Microsoft también ha publicado un [índice de explotabilidad](#) para ayudar a los clientes a comprender la probabilidad de explotación. Esta puede ser información útil para quienes necesitan ayuda con la priorización de actualizaciones de seguridad. Como advertencia, esta información refleja la probabilidad de explotación en el momento en que se publicó la actualización de seguridad. Puede que no refleje la explotabilidad en el mundo real que se desarrollará en las próximas semanas o meses a medida que más actores de amenazas utilicen la vulnerabilidad como arma. El índice se utiliza mejor para priorizar actualizaciones a muy corto plazo, en lugar de como justificación para retrasar significativamente la aplicación de parches.

Índice de Explotabilidad de Microsoft

Fig. 3: El [Índice de explotabilidad de Microsoft](#) evalúa la probabilidad de explotación en el momento en que se publicó la actualización de seguridad

Índice	Definición Corta	Definición Completa
0	Explotación Detectada	Microsoft tiene conocimiento de un caso en el que se está explotando esta vulnerabilidad. Como tal, los clientes que revisaron la actualización de seguridad y determinaron su aplicabilidad dentro de su entorno deben tratar esto con la máxima prioridad.
1	Explotación más Probable	El análisis de Microsoft ha demostrado que el código de explotación podría crearse de tal manera que un atacante pudiera aprovechar esta vulnerabilidad de forma consistente. Además, Microsoft es consciente de casos pasados en los que se ha aprovechado este tipo de vulnerabilidad. Esto lo convertiría en un objetivo atractivo para los atacantes y, por lo tanto, sería más probable que se pudieran crear exploits. Como tal, los clientes que revisaron la actualización de seguridad y determinaron su aplicabilidad dentro de su entorno deben tratar esto con mayor prioridad.
2	Explotación menos Probable	El análisis de Microsoft ha demostrado que, si bien se podría crear un código de explotación, un atacante probablemente tendría dificultades para crear el código, lo que requeriría experiencia y/o sincronización sofisticada, y/o resultados variados al atacar el producto afectado. Además, Microsoft no ha observado recientemente una tendencia de que este tipo de vulnerabilidad se explote activamente. Esto lo convierte en un objetivo menos atractivo para los atacantes. Dicho esto, los clientes que revisaron la actualización de seguridad y determinaron su aplicabilidad dentro de su entorno aún deben tratarla como una actualización importante. Si están priorizando otras vulnerabilidades altamente explotables, podrían clasificarlas más abajo en su prioridad de implementación.
3	Explotación Improbable	El análisis de Microsoft muestra que es poco probable que un código de explotación que funcione correctamente se utilice en ataques reales. Esto significa que, si bien es posible que se publique un código de explotación que pueda desencadenar la vulnerabilidad y causar un comportamiento anormal, el impacto total de la explotación será más limitado. Además, Microsoft no ha observado casos de este tipo de vulnerabilidad que se hayan explotado activamente en el pasado. Por lo tanto, el riesgo real de ser explotado por la vulnerabilidad es significativamente menor. Dicho eso, los clientes que hayan revisado la actualización de seguridad para determinar su aplicabilidad dentro de su entorno podrían priorizar esta actualización por debajo de otras vulnerabilidades dentro de una versión.



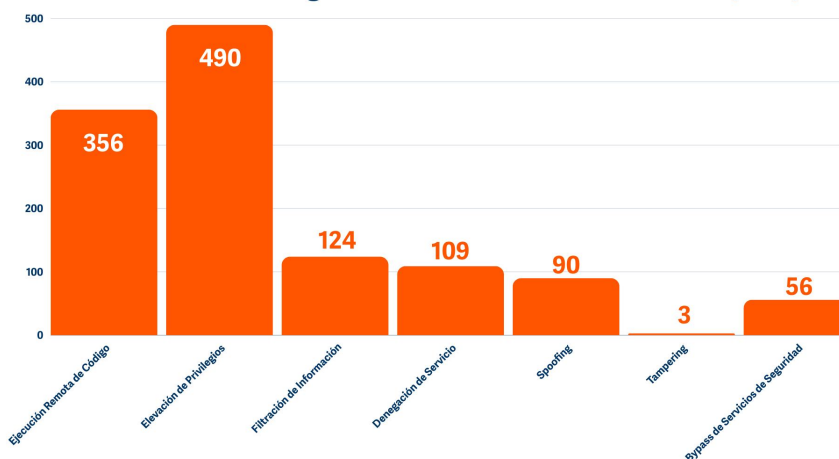
Análisis de las Vulnerabilidades

Vulnerabilidades por Categoría

Cada boletín de seguridad de Microsoft se compone de una o más vulnerabilidades, que se aplican a uno o más productos de la empresa.

Microsoft normalmente agrupa las vulnerabilidades en estas categorías principales: Ejecución Remota de Código (RCE), Elevación de Privilegios (EoP), Filtración de Información, Denegación de Servicio (DDoS), Spoofing, Tampering y Bypass de Servicios de Seguridad.

Clasificación de las Categorías de Vulnerabilidad de Microsoft (2023)



La Elevación de Privilegios sigue siendo la primera categoría de vulnerabilidad, a pesar de una caída significativa del 31% de 715 a 490 respecto al año anterior.

Microsoft Vulnerability Categories (2019-2023)

	2019	2020	2021	2022	2023
Remote Code Execution	323	345	326	314	356
Elevation of Privilege	198	559	588	715	490
Information Disclosure	177	179	129	114	124
Denial of Service	52	46	55	72	109
Spoofing	63	104	66	31	90
Tampering	8	7	3	4	3
Security Feature Bypass	38	30	44	42	56

La Ejecución Remota de Código rompe su tendencia a la baja en 2023, aumentando un 13% hasta 356, el número más alto que hemos visto desde el debut de este informe.

La ejecución remota de código y la elevación de privilegios siguen siendo las principales categorías de vulnerabilidad, lo que una vez más resalta los objetivos de los actores de amenazas.

La Elevación de Privilegios Sigue Siendo Categoría #1 de Vulnerabilidades en 2023

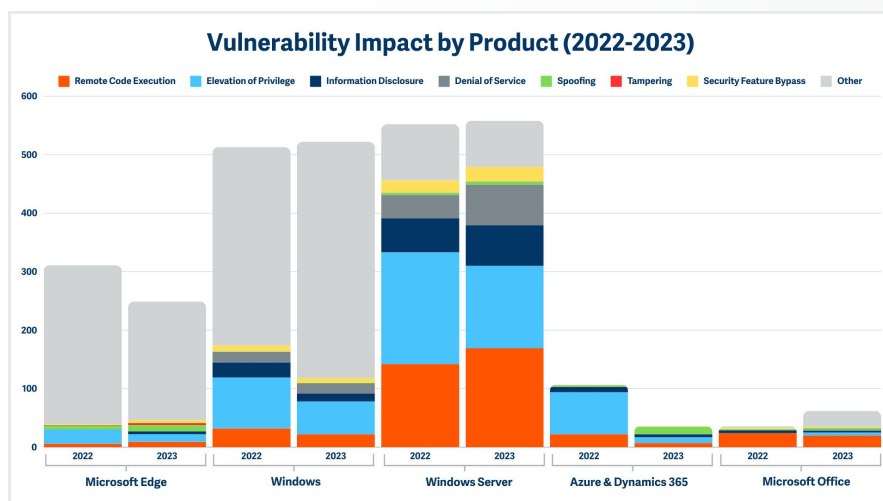
La Elevación de Privilegios ha continuado su tendencia posterior a 2019 y sigue siendo la categoría #1 de vulnerabilidades en 2023, seguida de la Ejecución Remota de Código. Esto no es sorprendente, ya que tiene un paralelo directo con tácticas de amenaza conocidas.

Dos tácticas principales de los actores de amenazas son:

1. Hacer que su código se ejecute (<https://ataque.mitre.org/tactics/TA0002/>)
2. Obtener acceso a los privilegios necesarios para cumplir con sus objetivos (<https://attack.mitre.org/tactics/TA0004/>)

La buena noticia de este año es que, si bien las vulnerabilidades de elevación de privilegios siguen siendo la categoría de vulnerabilidades #1, han disminuido de 715 a 490, una caída sustancial del 31%. Cuando profundizamos en los datos, podemos ver claramente que esas reducciones provienen principalmente de las vulnerabilidades de Azure y Windows Server, como se muestra en la siguiente figura.

Esta es una buena noticia, dado que estos sistemas suelen ser públicos y es mucho más probable que contengan grandes cantidades de datos confidenciales y cuentas de servicios privilegiados que, por ejemplo, un sistema Windows Desktop.



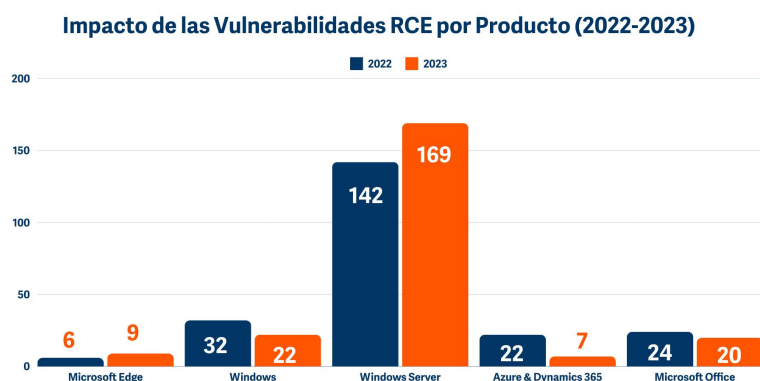
Azure y Windows Server muestran una reducción significativa en las vulnerabilidades de EoP. Azure cayó de 72 vulnerabilidades EoP en 2022 a 10 en 2023 (una enorme disminución del 86%) y Windows Server cayó de 191 a 141 (reducción del 26%).

En general, la reducción de las vulnerabilidades de elevación de privilegios es una tendencia muy positiva que reduce directamente las opciones de un atacante al implementar una amenaza que requiere privilegios elevados para ejecutarse.

Sin embargo, no se puede confiar simplemente en la falta de vulnerabilidades de elevación de privilegios para proteger el acceso a los privilegios. Aún es esencial mantener una estrategia sólida de gestión de accesos privilegiados para eliminar y proteger privilegios dentro de un entorno para evitar que caigan en manos de un atacante.

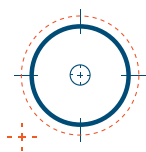
La Ejecución Remota de Código le Sigue de Cerca a la Elevación de Privilegios en 2023

En segundo lugar se encuentra la categoría de vulnerabilidades de Ejecución Remota de Código (RCE), que aumentó 13% (de 314 a 356 en 2023). Si bien en muchas áreas de productos, como Azure, Office y Windows (que ahora consisten principalmente en datos de Windows 10 y 11), hemos visto una disminución del RCE. Esto se vio compensado este año por un aumento en Windows Server.



Las vulnerabilidades de RCE en Windows Server aumentaron un 19% (de 142 a 169 en 2023).

El aumento de las vulnerabilidades de RCE en el sistema Windows Server no es causado por un componente en particular, sino que se distribuye ampliamente entre diferentes servicios y características. De hecho, muchas de estas detecciones fueron el resultado de la mayor colaboración de Microsoft con su comunidad de investigación de seguridad. En particular, parece que esta colaboración está dando sus frutos porque muchas de estas vulnerabilidades se revelaron directamente a Microsoft y se parchearon antes de que se divulgaran públicamente o se observara su explotación.

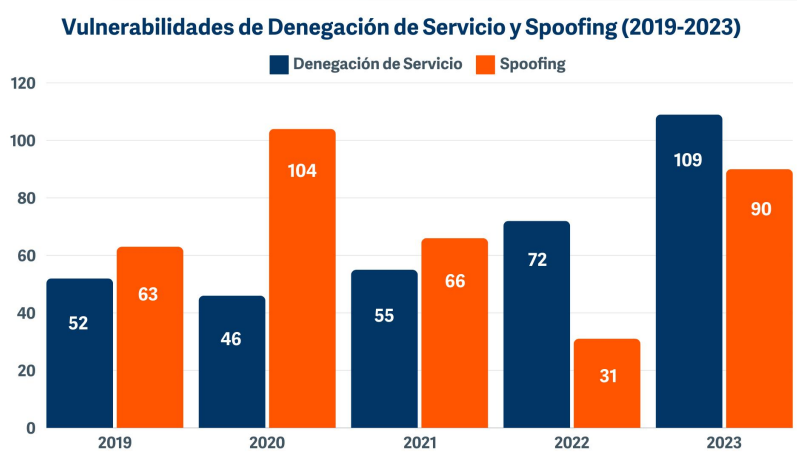


Riesgo, ingeniería inversa e investigadores: la carrera continúa.

Los parches oportunos permiten a las organizaciones mantenerse por delante de la mayoría de los actores de amenazas, siempre que las organizaciones implementenlos de manera oportuna. Una vez que se revela una vulnerabilidad y se lanzan los parches, comienza la carrera para parchear con éxito antes de que un actor de amenazas realice ingeniería inversa en el parche o la vulnerabilidad se divulgue públicamente, lo que permite la creación de exploits.

Tanto los investigadores como los actores de amenazas han tenido éxito en parches de ingeniería inversa para encontrar soluciones alternativas explotables u otras vulnerabilidades en áreas de código parcheadas recientemente. Como dice el refrán, no hay humo sin fuego y, como destacamos en el informe del año pasado, las vulnerabilidades pueden comenzar a multiplicarse cuando se llama la atención sobre un área que podría contener múltiples áreas de código explotables.

Las Vulnerabilidades de Denegación de Servicio y Spoofing aumentarán significativamente en 2023



Las vulnerabilidades de Denegación de Servicio alcanzaron un récord en 2023, aumentando un 51%, de 72 en 2022 a 109 en 2023, y el Spoofing demostró un espectacular aumento del 190%, de 31 en 2022 a 90 en 2023.

Cuando pensamos en la seguridad de la información, a menudo nos centramos en garantizar la confidencialidad y la integridad de los datos, pero alterar la disponibilidad de los datos también puede tener un impacto devastador. Los exploits de denegación de servicio (DoS) se pueden utilizar para interrumpir la disponibilidad de datos y provocar desafíos a los negocios de forma similar al ransomware.



¿Qué podemos aprender de las categorías de vulnerabilidades de este año?

A medida que las vulnerabilidades generales se estabilizan, los actores de amenazas cambian su atención a las identidades.

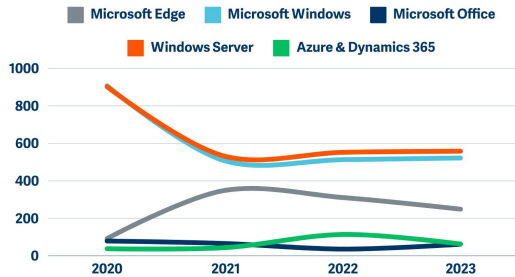
Cuando se trata de ejecutar código, los actores de amenazas tienen opciones más allá de explotar las vulnerabilidades. Pueden utilizar ingeniería social o credenciales robadas para introducir su código en un entorno sin necesidad de una vulnerabilidad de software. De manera similar, cuando se trata de elevar privilegios, podría ser más fácil secuestrar una cuenta que ya tiene privilegios que explotar una vulnerabilidad de software o una mala configuración en el entorno para acceder a los privilegios necesarios.

A medida que el número total de vulnerabilidades de Microsoft se estabiliza y el número de vulnerabilidades críticas disminuye, vemos que los atacantes, al igual que el agua, fluirán hacia el camino de menor resistencia y centrarán mucho más su atención en las identidades.

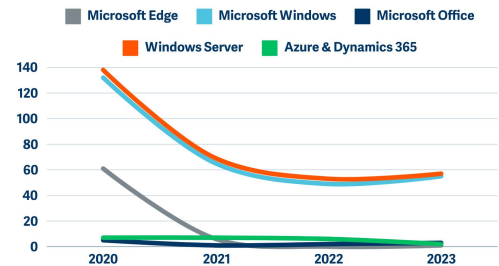
Sin embargo, esto no significa que podamos volvernos complacientes con las vulnerabilidades del software. No sólo hay muchas vulnerabilidades para todos, sino que también hay una serie de sistemas sin parches que aún son vulnerables a exploits para los que se pusieron parches disponibles hace meses o años. Estas vulnerabilidades conocidas hacen que sea muy fácil para los actores de amenazas lanzar un ataque exitoso.

Vulnerabilidades por Producto

Vulnerabilidades por Producto (2020-2023)

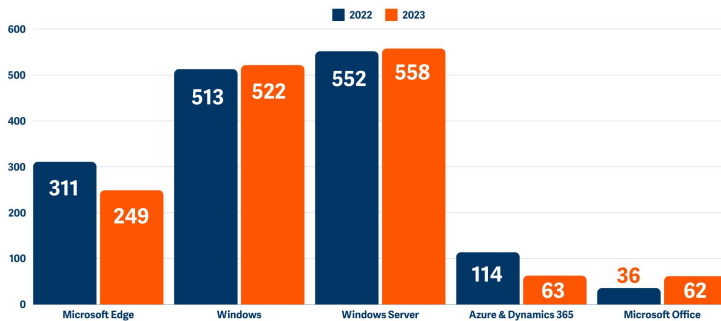


Vulnerabilidades Críticas por Producto (2020-2023)



En general, las cifras de vulnerabilidad se han estabilizado. Las vulnerabilidades totales continúan estancadas desde hace cuatro años y las vulnerabilidades críticas continúan disminuyendo, aunque el descenso se ha desacelerado.

Vulnerabilidades de Microsoft por Producto (2022-2023)



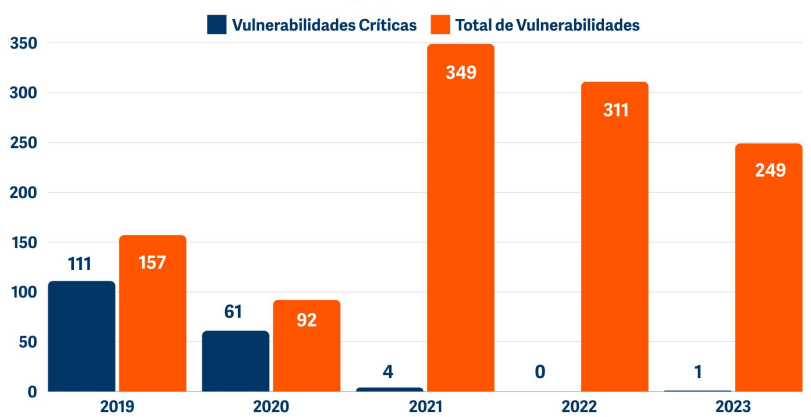
Las vulnerabilidades de Windows Server aumentaron ligeramente en 2023. El número total aumentó ligeramente de 552 a 558 (1%), y las críticas experimentaron un ligero aumento similar, de 53 a 57.

Las vulnerabilidades de Windows mostraron un patrón similar, con el total aumentando de 513 a 522 (2%), y las críticas aumentando de 49 a 55.

Office y Edge continúan líderes, y Azure corrige el rumbo después de un pico sin precedentes en 2022.

Microsoft Edge continúa la tendencia a la baja de vulnerabilidades

Vulnerabilidades de Microsoft Edge (2019-2023)*



La base de código de Chromium continúa ofreciendo importantes mejoras de seguridad, marcadas por una caída en picado de vulnerabilidades y exploits en tres años.

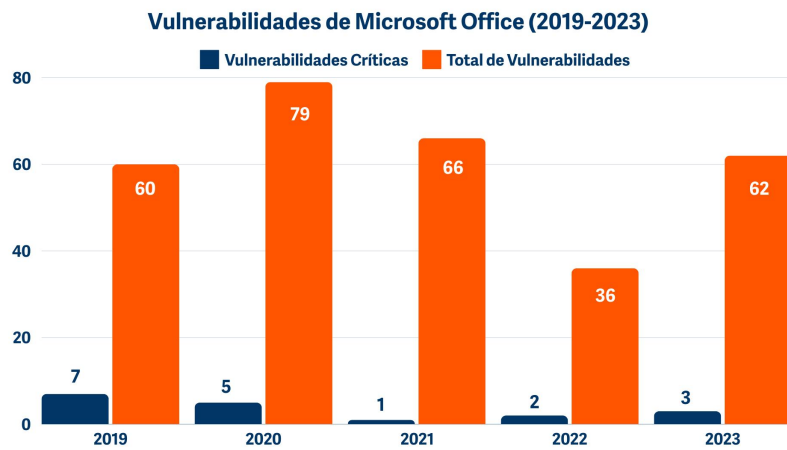
*2019-2021 incluye Internet Explorer, que se discontinuó el año pasado. Las cifras de 2022/23 son solo para Edge.

Los navegadores web y los visores de documentos han sido históricamente un gran problema en lo que respecta a vulnerabilidades y ciberataques. Afortunadamente, Microsoft ha logrado avances significativos en la maduración de la seguridad de estas áreas.

En el lado del navegador, alejar Edge de una base de código personalizada de Microsoft y pasarla a una base de código Chromium produjo importantes mejoras de seguridad. Eliminar la compatibilidad con Internet Explorer también ha ayudado, haciendo que los exploits de descarga no autorizada y los complementos Flash vulnerables sean cosa del pasado.

Las vulnerabilidades críticas en Microsoft Edge se han desplomado desde 162 en 2017 a solo 1 en 2023 (y 0 en 2022). Esto se debe en gran medida a la adopción de la madurez de seguridad que ofrece Chromium, que se utiliza como base para múltiples navegadores web.

Las vulnerabilidades de Microsoft Office vuelven a los niveles de 2019-2021 en 2023



Las vulnerabilidades de Office aumentan a lo largo de 2022, pero continúan una tendencia general a la baja, lo que obliga a los atacantes a utilizar métodos de ataque más innovadores.

En el caso de Office, hemos visto una tendencia a la baja similar (aunque no tan dramática) tanto para el número total de vulnerabilidades como para las críticas, a pesar de un aumento en 2023. Esto se debe en parte a que algunas de las versiones anteriores de Office están llegando al final de su vida útil (EoL) y ya no son compatibles.

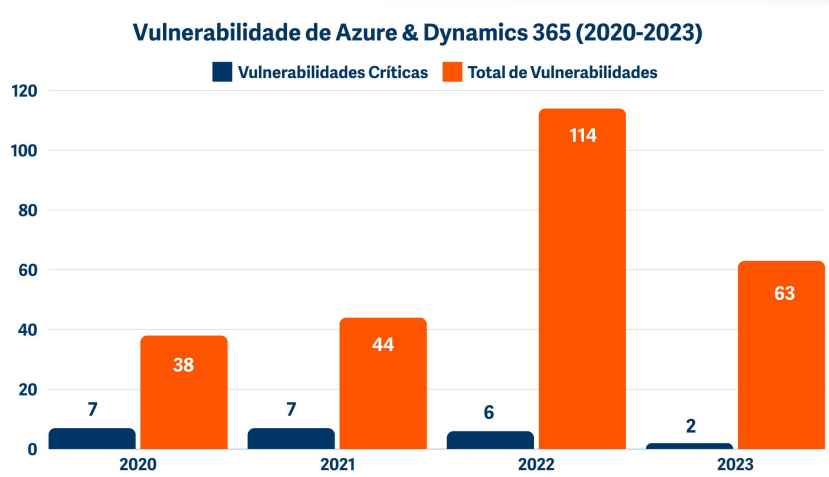
Esfuerzos para prevenir el phishing y las cargas útiles de malware a través de aplicaciones de Office continúan obligando a los atacantes a innovar. Los controles para desactivar la ejecución automática de macros en documentos descargados han bloqueado algunas rutas comunes hacia la ejecución remota de código, lo que ha obligado a los actores de amenazas a buscar formas más creativas de ejecutar código utilizando documentos y archivos maliciosos.

Una de las nuevas áreas más interesantes para las vulnerabilidades dentro de las aplicaciones de Office proviene de la adición de soporte por parte de Microsoft para los archivos SKP patentados de SketchUp Software en junio de 2022. Esto fue diseñado para facilitar la importación de modelos 3D a Word, Excel, PowerPoint y Outlook. Lamentablemente, agregar compatibilidad con archivos 3D a los documentos también introdujo una nueva dimensión en el panorama de las vulnerabilidades, según el equipo de [ThreatLabz](#) que descubrió 117 vulnerabilidades únicas que se acumularon en CVE-2023-33146, CVE-2023-28285 y CVE-2023-29344.

Microsoft creó un parche para abordar estas vulnerabilidades, que el equipo de ThreatLabz pudo evitar. Esto provocó que Microsoft deshabilitara temporalmente la compatibilidad en Microsoft 365 para archivos SketchUp en junio de 2023.

Si bien Microsoft ha admitido formatos de archivos 3D desde hace un tiempo, este incidente refuerza cómo cualquier adición de las nuevas funciones pueden introducir vulnerabilidades de seguridad. En este caso, el código adicional agregado a la biblioteca DLL MSOSPECTRE, que es responsable de analizar formatos de archivos 3D, expuso vulnerabilidades que Microsoft no había previsto.

Las vulnerabilidades de Azure y Dynamics 365 casi se redujeron a la mitad en 2023.



Después de aumentar en 2022, las vulnerabilidades de Azure y Dynamics 365 experimentaron una impresionante disminución del 45%: de 114 a 63 en 2023.

Después de que las vulnerabilidades de Microsoft Azure y Dynamics 365 se dispararan en 2022, se redujeron casi a la mitad en 2023: de 114 a 63. Teniendo en cuenta la gran cantidad de productos y servicios que cubre esta área de productos, las cifras son impresionantemente bajas.

En el [informe del año pasado](#), destacamos una herramienta de migración a la nube que causó una proporción sustancial de las vulnerabilidades en gran medida, asociada con vulnerabilidades de tipo SQLi (¿quién hubiera pensado que todavía estaríamos hablando de SQLi hoy!).

En 2023, esta tendencia ascendente se ha corregido y ha vuelto al nivel que esperaríamos ver. Esta área de productos es predominantemente código más nuevo que se desarrolla íntegramente utilizando el ciclo de vida de desarrollo seguro de Microsoft, y podemos ver claramente los beneficios en comparación con los productos heredados, que generalmente tienen tasas más altas de vulnerabilidades.

"El refuerzo proactivo de la seguridad a menudo rompe la cadena de explotación del atacante, evitando que una sola cuenta suplantada le dé al atacante un administrador de dominio."

**Jay Beale, Director Ejecutivo Y De Tecnología,
InGuardians, Inc.**



Vulnerabilidades Destacadas



Comprender los métodos que utilizan los actores de amenazas para explotar vulnerabilidades e infiltrarse en las organizaciones puede ayudarle a tomar decisiones más informadas para proteger su empresa.

La Bola de Nieve de Print Spooler se Ralentiza

La fiebre de las vulnerabilidades - y objetivos principales de los ataques de Elevación de Privilegios - puede estar llegando a su fin, pero eso no significa que los actores de amenazas no puedan seguir sacando provecho.

2018

Se identifica "el Printer Bug". Este error permite que un usuario sin privilegios en la red active de forma remota el servicio Print Spooler del controlador de dominio para autenticarse en un sistema arbitrario. Este error permite al atacante hacerse pasar por el controlador de dominio.

2019

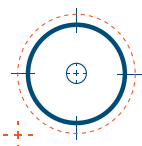
"El Printer Bug" se convierte en [CVE-2019-0683](#) y llama la atención sobre el Print Spooler.

2020

Se revelan siete (7) vulnerabilidades de elevación de privilegios de [Printer Spooler](#). Inicialmente, todas estas vulnerabilidades son vectores de ataque locales, lo que requiere que el atacante primero tenga acceso directo al sistema que ejecuta Print Spooler. Sin embargo, el resultado de cada uno de ellos es que un atacante podría ejecutar código arbitrario con privilegios elevados del sistema.

[CVE-2020-1030](#)
[CVE-2020-1048](#)
[CVE-2020-1070](#)
[CVE-2020-1337](#)
[CVE-2020-17001](#)
[CVE-2020-17014](#)

[CVE-2020-17042](#)
Aparecerá a finales de 2020. A diferencia de exploits anteriores que se podían explotar localmente, este se puede explotar de forma remota, lo que significa que el atacante sólo necesita estar en la red. Este atributo de RCE hace que esta vulnerabilidad particular sea mucho más grave. Sin embargo, esta vulnerabilidad no se había divulgado públicamente y no se sabía que se utilizara como un exploit antes de que se parcheara.



El Efecto Bola de Nieve de las Vulnerabilidades

Este fenómeno ocurre cuando se encuentra y parchea una vulnerabilidad, pero el proceso atrae el nuevo escrutinio de nuevos investigadores que encuentran nuevas vulnerabilidades, nuevos vectores de ataque y nuevas formas de solucionar parches anteriores, lo que hace que el recuento de vulnerabilidades aumente como una bola de nieve.

El servicio Print Spooler, que contiene código que tiene más de 20 años, es un ejemplo del efecto bola de nieve de vulnerabilidad en acción.

**2021**

Se revelan 16 vulnerabilidades de elevación de privilegios de Print Spooler. El Print Spooler ahora está captando la atención de muchos investigadores como una forma interesante de realizar ataques de Elevación de Privilegios.

La cantidad de vulnerabilidades EoP de Windows Print Spooler reveladas aumenta rápidamente a medida que Microsoft juega Whack-A-Mole con investigadores que han encontrado formas de solucionar parches y continúan explotando vulnerabilidades.

CVE-2021-. 34527 es la más notable de la clase 2021 de vulnerabilidades EoP de Windows Print Spooler.

Esta vulnerabilidad es muy sencilla de explotar.

Una red necesitaba de una cuenta de usuario válida y el Print Spooler para permitir conexiones remotas (que están habilitadas de forma predeterminada). La facilidad de explotación, combinada con el hecho de que se había divulgado públicamente le valió el nombre de "Print Nightmare."

Las otras 15 vulnerabilidades de la clase 2021 incluyen:

CVE-2021-41333, CVE-2021-41332, CVE-2021-40447, CVE-2021-38671, CVE-2021-38667, CVE-2021-36970, CVE-. 2021-36958, CVE-2021-36947, CVE-2021-36936, CVE-2021-34483, CVE-2021-34481, CVE-2021-26878, CVE-2021-1695, CVE-2021-1675 y CVE-2021-1640

2022

Se revelan 35 vulnerabilidades de elevación de privilegios de Print Spooler, más del doble de lo registrado el año anterior.

CVE-2022-44681, CVE-2022-44678, CVE-2022-41073, CVE-2022-38028, CVE-2022-38005, CVE-2022-35793, CVE-2022-30226, CVE-2022-30206, CVE-. 2022-30138, CVE-2022-29140, CVE-2022-29132, CVE-2022-29114, CVE-2022-29104, CVE-2022-26803, CVE-2022-26802, CVE-2022-26801, CVE-2022-. 26798, CVE-2022-26797, CVE-2022-26796, CVE-2022-26795, CVE-2022-26794, CVE-2022-26793, CVE-2022-26792, CVE-2022-26791, CVE-2022-26790,. CVE-2022-26789, CVE-2022-26787, CVE-2022-26786, CVE-2022-23284, CVE-2022-22718, CVE-2022-22717, CVE-2022-22041, CVE-2022-22022, CVE-. 2022-21999 y CVE-2022-21997

2023

Se revelan 5 vulnerabilidades de elevación de privilegios de Print Spooler, una reducción significativa con respecto a años anteriores.

CVE-2023-35325, CVE-2023-35302, CVE-2023-21765, CVE-2023-21760, CVE-2023-21678

En el informe del año pasado, hablamos sobre el efecto bola de nieve en torno a las vulnerabilidades de Print Spooler, donde el código de más de 20 años que se había transmitido a través de las versiones de Windows había comenzado a mostrar su edad y convertirse en una meta para los exploits. Las vulnerabilidades de Print Spooler se habían duplicado aproximadamente cada año desde el descubrimiento en 2019 de "The Printer Bug" CVE-2019-0683, alcanzando su punto máximo en 2022 con 35 vulnerabilidades.

Esta fiebre parece ahora se haber reducido a cinco vulnerabilidades en 2023: [CVE-2023-35325](#), [CVE-2023-35302](#), [CVE-2023-21765](#), [CVE-2023-21760](#), [CVE-2023-21678](#)

Por muy alentador que sea ver cómo se reduce el volumen, estas son vulnerabilidades no insignificantes, y la mayoría está asociada con la elevación de privilegios. Dado que el servicio de Print Spooler se ejecuta como SYSTEM (el nivel más alto de privilegios en el sistema Windows), es una meta para los exploits de elevación de privilegios.

A diferencia de años anteriores, parece que Microsoft logró publicar parches antes de que cualquiera de estas vulnerabilidades fuera divulgada públicamente o explotada. Esto proporciona cierta tranquilidad de que se han aprendido lecciones en esta área, pero aún demuestra que ahora no es el momento de volverse complacientes.

Es hora de decir "adiós"

Software al final de su vida útil (EOL) ya no cuenta con soporte ni parches, lo que lo convierte en un riesgo elevado para las empresas y un objetivo para los actores de amenazas.

Muchos productos de Microsoft alcanzaron su fin de vida útil (EOL) en 2023. Esto significa que ya no recibirán parches de seguridad para abordar vulnerabilidades u otros problemas.

Este año destaca el EOL de Server 2012 y Server 2012R2. Como regalo de despedida, ambos sistemas operativos recibieron un paquete de retiro de 65 parches, 11 de los cuales eran críticos. Para incentivar las migraciones de la nube a Azure para quienes aún usan estos SOs, Microsoft ofrece tres años de actualizaciones de seguridad extendidas (ESU) más allá del final de la fecha de soporte (octubre de 2023) en Azure.

En el otro extremo del programa de actualizaciones de seguridad extendidas (ESU) de Microsoft se encuentra Windows 7, el sistema operativo que probablemente ya pensaba que había desaparecido hace mucho tiempo ya no está cubierto por el programa ESU de Microsoft. Dado que esto significa que no habrá más acceso a parches de seguridad críticos, definitivamente es hora de acelerar los planes para hacer avanzar cualquier sistema Windows 7 heredado.

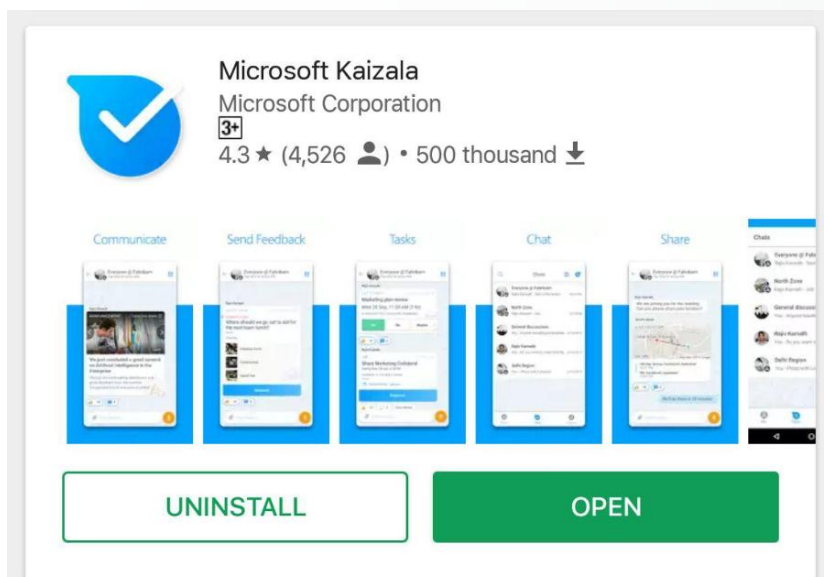


Fig. 4: Microsoft Kaizala es uno de los muchos productos que alcanzarán su final de vida útil (EOL) en 2023.

También hubo algunos productos que, al igual que el mp3 Microsoft Zune, no lograron despegar y fueron retirados sin mucha atención. Entonces, en 2023, nos despedimos de Microsoft Kaizala. Su mensajería ahora forma parte de Teams y se ha visto obligada a retirarse.

Outlook no tiene suerte con CVE-2023-23397

Una combinación peligrosa de facilidad de explotación y alto impacto hizo que esta vulnerabilidad llamara la atención de los administradores de TI (y de los actores de amenazas) en 2023

Si bien continuamos celebrando un mínimo histórico de vulnerabilidades críticas en los productos de Microsoft, todavía hay algunas que preocuparon a los profesionales de TI en 2023.

A diferencia de muchas vulnerabilidades anteriores, CVE-2023-23397 en Microsoft Outlook no requiere interacción del usuario para activar el exploit. Peor aún, la vulnerabilidad afectó a todas las versiones de Outlook para Windows y permitió a un atacante obtener hashes de credenciales sensibles de Windows New Technology LAN Manager (NTLM). Esta peligrosa combinación de facilidad de explotación y alto impacto resultó en una puntuación CVSS de 9.8, que es más que suficiente para llamar la atención tanto de los administradores de TI como de los actores de amenazas.

La vulnerabilidad se activa cuando un atacante envía una invitación o cita de calendario al correo electrónico de la víctima. Esta invitación contiene propiedades adicionales que hacen que Outlook establezca una conexión SMB y active la autenticación NTLM en un servidor en Internet que está bajo el control del atacante. A partir de ahí, el atacante puede capturar los hashes NTLM y usarlos para autenticarse como víctima, lo que lleva a una posible escalada de privilegios y un mayor compromiso del entorno.

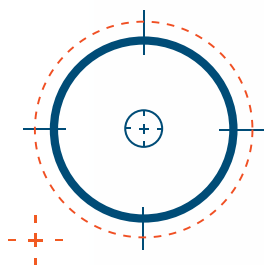
El peligro real es que la vulnerabilidad se activa sin que el usuario tenga que abrir la invitación. De hecho, el desencadenante es el sonido de notificación de recordatorio.

Si bien este suele ser un sonido de "ping" predecible para recordarle que está a punto de realizarse una reunión, existe una propiedad "PidLidReminderFileParameter" que se puede usar para especificar un archivo de audio personalizado para reproducir. Se puede abusar de esta propiedad. Si un atacante lo configura como un recurso remoto bajo su control, Outlook se conectará y autenticará, lo que finalmente revelará los hash de las credenciales de la víctima. Como destacamos en el informe del año pasado, vulnerabilidades impactantes como esta, a menudo, llaman la atención tanto de los actores de amenazas como de la comunidad de investigación, lo que resulta en un juego de Whack-A-Mole mientras Microsoft intenta lanzar parches más rápido de lo que se descubren las soluciones. El experto Dominic Chell [descubrió rápidamente](#) que el parche lanzado para CVE-2023-23397 solo solucionaba el problema del acceso remoto, y si un atacante estuviera dentro de la red, aún estaría capaz de explotar esta vulnerabilidad.

Si bien hay mitigaciones disponibles, como bloquear conexiones SMB o agregar usuarios al grupo de protegidos para evitar el uso de la autenticación NTLM, esto es una vulnerabilidad crítica que hay que parchear dada la facilidad con la que se puede explotar.

Debido a que la vulnerabilidad permite a un atacante capturar y reproducir hashes NTLM para autenticarse como víctima, **es importante respetar siempre el principio de privilegio mínimo. Cuantos menos privilegios tenga la víctima, menor será el riesgo de que su cuenta y su identidad se vean comprometidas.**

En el peor de los casos, un administrador de dominio revisaría los correos electrónicos de una cuenta con privilegios elevados, lo que proporciona al atacante un camino fácil para hacerse cargo de todo el dominio. En un escenario ideal, habría eliminado los privilegios de administrador local y habría protegido adecuadamente las cuentas con privilegios elevados, como las de administradores de dominio, para garantizar que, sin importar qué vulnerabilidad se explotara, los impactos se mitigarían.



Es importante respetar siempre el principio de privilegio mínimo. Cuantos menos privilegios tenga la víctima, menor será el riesgo de que su cuenta y su identidad se vean comprometidas.

La RomCom Rusa no Da en el Blanco con CVE-2023-36884

Estas elaboradas campañas de phishing se dirigieron a entidades gubernamentales y de defensa con archivos maliciosos que aprovecharon un exploit de ejecución remota de código de día cero para evadir las protecciones del Mark of the Web. Este es un claro ejemplo de cómo los atacantes han sido innovadores al eludir las protecciones mientras Microsoft continúa mejorando la seguridad de Office.

Una campaña de phishing en 2023, atribuida al grupo **cibercriminal ruso** RomCom (también conocido como Storm-0978), apuntó a entidades gubernamentales y de defensa en Europa y América del Norte con señuelos relacionados con el Congreso Mundial de Ucrania.

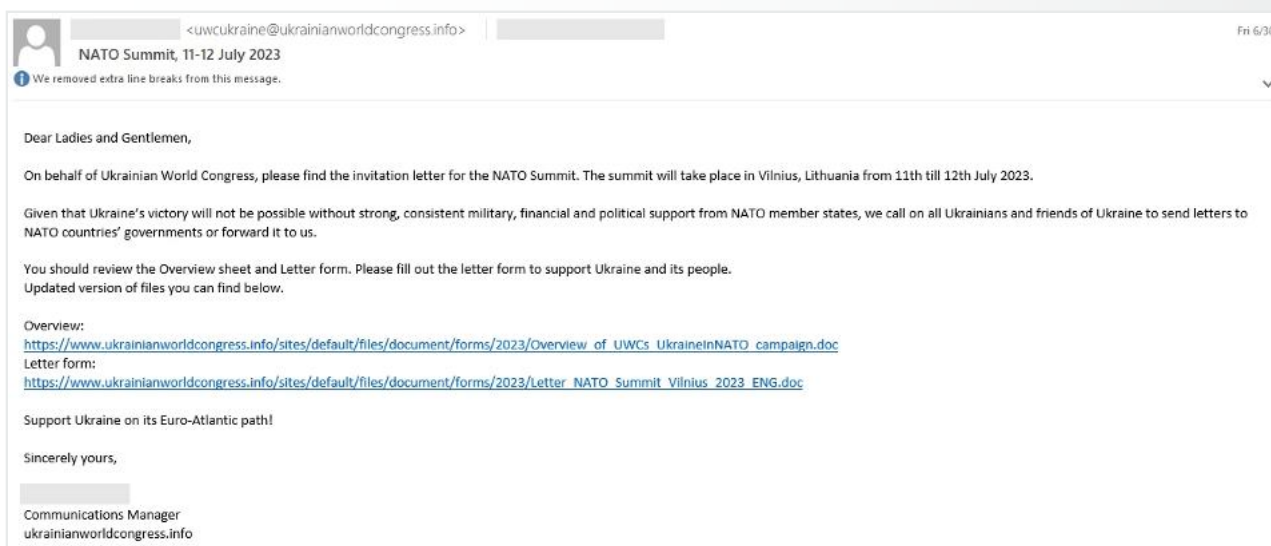


Figura 5: Una captura de pantalla de la campaña de phishing de 2023 lanzada por el grupo cibercriminal ruso RomCom

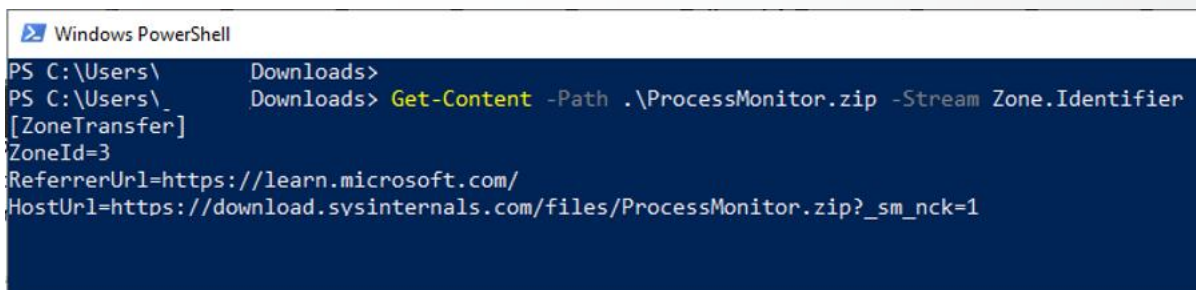
El objetivo del phishing era manipular a sus objetivos para que descargaran y abrieran los documentos maliciosos vinculados desde el correo electrónico.

Vale la pena señalar que los atacantes a menudo separan la carga maliciosa del correo electrónico de phishing mediante enlaces o en un documento adjunto. Esto hace que el malware sea más difícil de detectar porque el código malicioso está oculto dentro del correo electrónico. Cuando se analiza el e-mail y las soluciones de seguridad intentan escanear estos enlaces, el servidor que aloja las cargas puede bloquearlos o redirigirlos.

RomCom es especialista en este tipo de ataques de phishing. El grupo comprometió una cuenta de correo electrónico del Ministerio de Defensa de Ucrania a finales de 2022. Su propósito durante este ataque era enviar correos de phishing con archivos adjuntos en formato PDF que contienen enlaces a sitios web comprometidos que albergan malware para robar información.

Si bien el uso de documentos de Office maliciosos no es nada nuevo, esta campaña se destacó por explotar una vulnerabilidad que luego se conoció como CVE-2023-36884.

Para proteger a los usuarios contra documentos maliciosos, Microsoft adjunta un tag de identificación de zona, conocido como "Mark of the Web", a los archivos descargados por navegadores y clientes de correo electrónico. Este tag contiene un ID que indica si el archivo se descargó de Internet o de la red local, así como las URL desde las que se originó.



```
Windows PowerShell
PS C:\Users\Downloads>
PS C:\Users\Downloads> Get-Content -Path .\ProcessMonitor.zip -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://learn.microsoft.com/
HostUrl=https://download.sysinternals.com/files/ProcessMonitor.zip?_sm_nck=1
```

Figura 6 : Uso de PowerShell para mostrar el Mark of the Web en un archivo descargado.

Luego, Microsoft Office, Microsoft SmartScreen y otras herramientas de seguridad utilizan Mark of the Web (MotW) para aplicar restricciones, como evitar que macros potencialmente maliciosas en un documento de Word se ejecuten automáticamente.

En este caso, RomCom había descubierto un exploit de ejecución remota de código de día cero para evadir las protecciones de Mark of the Web. Explotaron una función de búsqueda de Windows para descargar archivos remotos en el sistema de archivos local donde, por un breve tiempo, no fueron etiquetados con MotW. Esto evitó efectivamente las protecciones de MotW, lo que permitió al atacante ejecutar acciones que normalmente se evitarían para el contenido descargado de Internet. Luego, los actores de amenazas pudieron iniciar una cadena de eventos que terminó en la ejecución de código arbitrario.

Curiosamente, la estructura de los documentos maliciosos utilizados por RomCom contiene elementos del [exploit Follina](#), (destacado en el informe del año pasado), con análisis que lo vinculan a CVE-2022-30190, una vulnerabilidad que también se utilizó para eludir los controles de seguridad de documentos de Office. A medida que Microsoft mejoró la seguridad de Office, los atacantes continuaron innovando para eludir las protecciones.

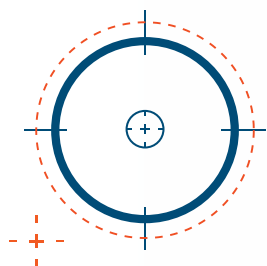
Este exploit no estaba solo. En 2023, investigadores de [Palo Alto Networks](#) también descubrieron [CVE-2023-36584](#), que utilizaba un vector de exploit diferente para evitar también MotW.

Este flujo constante de vulnerabilidades de ejecución remota de código en Office destaca que, incluso con estas recientes mejoras de seguridad de Microsoft, los atacantes siguen encontrando formas de ejecutar código.

Muchas empresas que luchan contra vulnerabilidades históricas de Office y características de seguridad que no están habilitadas de forma predeterminada pueden sentir que la batalla está perdida. Sin embargo, como ocurre con todas las vulnerabilidades de ejecución remota de código, el principio de privilegio mínimo es una medida defensiva clave.

En última instancia, no importa cuál sea el exploit, la carga útil del malware se ejecutará en el contexto del usuario que abrió el documento. Si ese usuario tiene privilegios de administrador, también los tendrá el actor de la amenaza.

Pero si eliminas los privilegios y la capa de control de aplicaciones, podrás mitigar las amenazas de forma proactiva, incluso cuando se utiliza un exploit de día cero.



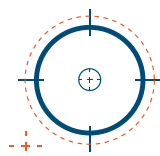
El principio de privilegio mínimo es una medida defensiva clave. No importa cuál sea el exploit, si elimina privilegios y capas de control de aplicaciones, puede mitigar las amenazas de manera proactiva, incluso cuando se utiliza un exploit de día cero.

¿Están las organizaciones atravesando una crisis de identidad?

Cada vez más, los atacantes están reenfocando sus esfuerzos en explotar identidades, en lugar de vulnerabilidades. Midnight Blizzard representa un excelente ejemplo de lo que puede suceder cuando los actores de amenazas se vuelven innovadores con tácticas de infiltración basadas en identidades.

Hace algún tiempo, Morey J. Haber, Chief Security Advisor de BeyondTrust, planteó la pregunta: "¿Estamos teniendo una crisis de identidad?". Al principio, el juego de palabras nos tomó por sorpresa, pero rápidamente nos dimos cuenta de que su pregunta era un juego de palabras basado en los crecientes desafíos que enfrentan las organizaciones en torno a la gestión y la seguridad de las identidades.

Como Chief Security Advisor y ex CSO y CTO, Morey ha estado rastreando la creciente ola de amenazas a las identidades, al mismo tiempo que ayuda a otros a comprender los complejos desafíos y el panorama de amenazas. Su nuevo libro, [Identity Attack Vectors: Strategically Designing and Implementing Identity Security](#), proporciona una evaluación exhaustiva de los desafíos de implementar una seguridad de identidades real dentro de una organización.



"[Su] crisis de identidad no es personal, sino que describe un problema con la forma en que gestiona las identidades y la seguridad de ellas en su organización"

Morey J. Haber,
Chief Security Advisor
BeyondTrust

Dado que este informe está diseñado para ayudar a las empresas a comprender mejor el panorama de amenazas en torno al ecosistema Microsoft, es importante abordar esta crisis de identidad y el hecho de que los atacantes están poniendo más énfasis en los vectores de ataque basados en ellas.

Cómo Identificar una Crisis de Identidad en su Ecosistema de Microsoft:

Preguntas Clave Basadas en Vectores de Ataque a las Identidades

¿Cómo se ve una crisis de identidad en el ecosistema Microsoft?

Un usuario inicia sesión, y eso es lo que lo hace tan difícil.

Puede tener sistemas completamente parcheados y excelentes herramientas de seguridad, pero si un atacante puede robar credenciales, secuestrar un token de sesión o usar técnicas de ingeniería social en la mesa de ayuda, es posible que pueda invadir su entorno. En un mundo donde es más fácil iniciar sesión que piratear, la identidad se convierte en el nuevo perímetro.

Vulnerabilidades, problemas de proceso y riesgos asociados con la identidad.

Los riesgos en sí se pueden diagnosticar identificando fallas en el proceso de entrada, salida y los permisos, privilegios, autenticación (como la autenticación multifactor (MFA), Single Sign On (SSO) y autorización para identidades y cuentas en reposo y operativas durante el tiempo de ejecución.

¿Qué convierte un desafío de seguridad en una crisis de identidad?

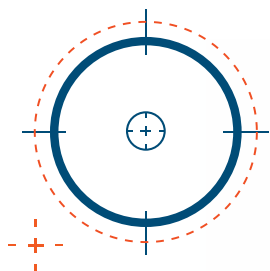
Las detecciones y recomendaciones necesarias para clasificar los riesgos generalmente están enterradas en lo profundo de los datos. Sin un enfoque clínico del problema, los síntomas a menudo pasan desapercibidos, a menos que un profesional esté específicamente buscando amenazas para ellos.

La mentalidad de muchos equipos de seguridad se han centrado en perseguir y detectar amenazas cuando, en realidad, es necesario volverse más proactivos. Cuando se trata de crisis de identidades, es posible que las vulnerabilidades no sean fallas en el código.

La vulnerabilidad podría deberse a una mala configuración en Active Directory que permite a cualquier usuario elevar sus privilegios. También podría ser una combinación de funciones oscuras de Entra ID que permiten a un atacante agregar credenciales a una aplicación OAuth privilegiada que puede acceder a las cajas de correo corporativos.

"La prevención es clave, y nunca se puede evitar todo. También es necesario detección."

Jay Beale, CEO Y CTO, InGuardians, Inc.



Los atacantes piensan en gráficos complejos para navegar por los sistemas de Microsoft

Hay un dicho bastante famoso en seguridad:

"Los defensores piensan en listas. Los atacantes piensan en gráficos. Mientras esto sea cierto, los atacantes ganan."

John Lambert,
Vicepresidente corporativo, Miembro de Seguridad,
Microsoft Security Research.

La idea es que un defensor piense en listas aisladas:

- El defensor A piensa en Active Directory,
- Defender B piensa en Windows Desktop AV,
- Defender C piensa en Windows Servers, etc.

El atacante, por otro lado, piensa en un gráfico, o una serie de conexiones entre cuentas y sistemas que puede utilizar para lograr su objetivo. Aprovechan la falta de visibilidad entre estos sistemas dispares (las listas de defensores) para moverse lateralmente e infligir daño. Eso podría significar comenzar en Windows Desktop con un administrador privilegiado local y luego usar ese acceso para capturar una cuenta de dominio con privilegios y pasar a un servidor.

Necesitamos poder pensar en gráficos, tal como lo hacen los atacantes. Si obtenemos una visibilidad integral de todas las cuentas, privilegios y accesos en nuestro entorno, podremos salir de nuestros silos y listas para ver qué ven los atacantes y qué pueden explotar en nuestros entornos.

Podemos comprender y corregir las rutas hacia los privilegios, las vulnerabilidades y las configuraciones incorrectas. Si bien es más fácil decirlo que hacerlo, es vital poder inclinar la balanza a favor de los defensores y adelantarse a las amenazas.

Como industria, debemos empezar a pensar de manera más integral sobre los privilegios y sobre la higiene y la detección de amenazas a las identidades .

Los mensajes principales que han resonado en este informe en los últimos 11 años (imponer privilegios mínimos, reforzar las configuraciones y la importancia de aplicar parches) representa algunas de las estrategias centrales necesarias para defenderse contra las amenazas cibernéticas. Estos mensajes centrales son igualmente aplicables a la crisis de identidades. No importa si una cuenta se ve comprometida a través de un secuestro de sesión en la nube o una vulnerabilidad explotada en un endpoint: cuantos menos privilegios y acceso tenga el usuario comprometido, más se reduce el riesgo.

Echemos un vistazo a cómo Microsoft se vio afectada por su propia crisis de identidad en 2023.

Microsoft es puesta a prueba por Midnight Blizzard

Los atacantes orchestaron un ataque magistral, aprovechando tácticas de infiltración basadas en identidades, privilegios y accesos a menudo inadvertidos para navegar a través de los sistemas de Microsoft. **El ataque Midnight Blizzard ejemplificó cómo es más fácil para los atacantes iniciar sesión con una cuenta robada que piratearla explotando una vulnerabilidad.**

Un excelente ejemplo de un ataque moderno basado en identidad ocurrió cuando Microsoft fue atacada por actores de amenazas conocidos como Midnight Blizzard (también Cozy Bear y APT29). Este ataque no parece haber involucrado ninguna de las vulnerabilidades que tradicionalmente cubrimos en este informe. En cambio, fue una clase magistral sobre **atacantes que piensan en gráficos** y utilizan privilegios y accesos a menudo inadvertidos entre cuentas y sistemas para navegar a través de los sistemas de Microsoft.

El ataque comenzó en 2023, cuando una cuenta en un entorno de prueba que no es de producción estuvo sujeta a un ataque de pulverización de contraseña. Desafortunadamente, la cuenta Entra ID objetivo no tenía habilitada la autenticación multifactor (MFA). Esto significaba que, una vez que los atacantes habían adivinado con éxito la contraseña, tenían acceso a la cuenta. Parece que la cuenta comprometida, aunque no tenía privilegios excesivos, tenía la capacidad de crear nuevos secretos para aplicaciones OAuth dentro del entorno de prueba. En este punto, el atacante debería haberse limitado al entorno de prueba, pero este no fue el caso. Microsoft declaró que, dentro del entorno de prueba, había una "aplicación OAuth heredada que tenía acceso elevado al entorno corporativo de Microsoft." Esto significaba que los atacantes tenían la capacidad de agregar secretos, autenticarse como aplicación de prueba privilegiada con acceso elevado al entorno corporativo y luego ejecutar comandos.

Con este amplio nivel de acceso, los atacantes podrían crear una nueva aplicación OAuth maliciosa y otorgarle el permiso "full_access_as_app" de Microsoft 365 Exchange Online para el entorno corporativo. Este permiso permitió al atacante acceder a los buzones de correo de altos ejecutivos utilizando credenciales asignadas a su aplicación OAuth maliciosa.

Este ataque es un ejemplo apropiado de cómo el panorama de amenazas está evolucionando hacia un punto de inflexión: **cada vez es más fácil para los atacantes iniciar sesión con una cuenta robada que hackearla explotando una vulnerabilidad.**

Como hemos demostrado en los 11 años que lleva publicándose este informe, el panorama está en constante evolución

Con las inversiones de Microsoft para proteger su software y reducir la cantidad de vulnerabilidades críticas, combinadas con el impulso a la nube para hacer que los datos y los sistemas sean accesibles desde cualquier red, **sólo podemos suponer que el volumen y la sofisticación de las amenazas a la seguridad de las identidades aumentarán sustancialmente en la próxima década.**

"Midnight Blizzard fue otro caso del dicho popular: 'Los atacantes no invaden, inician sesión'"

Jay Beale, CEO, CTO, InGuardians, Inc.

¿Qué dicen los expertos?

Paula Januszkiewicz



**CEO
CQURE**

Todos somos testigos de un cambio en la importancia de la ciberseguridad en la vida cotidiana. Durante mucho tiempo, ha sido una preocupación de los entusiastas de la tecnología. Hoy en día, se ha convertido en un aspecto vital de la realidad diaria tanto para individuos como para empresas. A medida que el mundo se vuelve cada vez más digital, lo que está en juego en la protección de nuestros datos y nuestra privacidad es mayor que nunca. Los conocimientos del Informe de vulnerabilidades de Microsoft 2024 de BeyondTrust sirven como recordatorio de los desafíos siempre presentes que enfrentamos.

Continúa en la página siguiente >



2023 fue el año de la IA, la IA generativa y la automatización, que seguirán revolucionando la forma en que abordamos la ciberseguridad en los próximos años. Estas tecnologías ofrecen un potencial increíble para detectar y mitigar amenazas, brindar apoyo en nuestras estrategias de defensa y hacer que el trabajo de los equipos de SecOps sea más manejable. Sin embargo, también introducen nuevos desafíos, como deepfakes y sofisticadas campañas de desinformación. La IA se ha convertido rápidamente en un arma de doble filo: una poderosa herramienta que sirve a ambas partes.

El Informe de vulnerabilidades de Microsoft de 2024 muestra una imagen matizada del estado actual de las vulnerabilidades. Como nota positiva, las vulnerabilidades críticas han experimentado una ligera disminución, continuando una tendencia esperanzadora. Además, el número de vulnerabilidades de elevación de privilegios (categoría principal de vulnerabilidad) se ha reducido sustancialmente, muy probablemente gracias al trabajo en las vulnerabilidades de Azure y Windows Server. Sin embargo, el número total de vulnerabilidades dentro del ecosistema de Microsoft se mantiene estable, una señal preocupante de que, a pesar de todos los esfuerzos e inversiones, el panorama de amenazas está lejos de disminuir. Destaca especialmente el marcado aumento de las vulnerabilidades de spoofing, lo que subraya la necesidad constante de vigilancia.

Refinar nuestro enfoque de la ciberseguridad es una tarea crucial. Esto incluye un control más estricto sobre los privilegios, reforzar los protocolos de seguridad y adaptar nuestras defensas a las características de nuestros entornos. La clave es mantenerse informado sobre las amenazas emergentes, implementar mecanismos eficaces de detección y respuesta, realizar periódicamente auditorías y pruebas de penetración, y revisar y probar continuamente nuestros planes de respuesta a incidentes. Estos principios resuenan profundamente con nuestras propias experiencias, reforzando su papel fundamental en el mantenimiento de un marco de ciberseguridad sólido.

Sin embargo, no debemos olvidar que en el corazón de la ciberseguridad sigue siendo el elemento humano. Las defensas tecnológicas más avanzadas pueden verse comprometidas por un simple error humano. Este informe señala un cambio que se está produciendo ahora: robar identidades es cada vez más fácil que explotar una vulnerabilidad. Como consecuencia, los ataques basados en las identidades serán aún más comunes en un futuro próximo.

Por lo tanto, es fundamental fomentar una cultura de concienciación y educación entre todos los usuarios. A diferencia del hacking, que suele ser un trabajo solitario, la ciberseguridad es un esfuerzo colaborativo. Esta perspectiva, de la que se hace eco el informe, destaca la importancia de un enfoque de la ciberseguridad centrada en las personas.

Al reflexionar sobre los conocimientos recopilados en el informe de BeyondTrust, está claro que el camino que tenemos por delante en 2024 nos exigirá adaptar y repensar nuestras estrategias de ciberseguridad. A medida que los adversarios se vuelven más sofisticados, será vital integrar más profundamente la ciberseguridad en nuestras rutinas diarias y operaciones del negocio. La clave para navegar el futuro será un enfoque equilibrado que combine la innovación tecnológica con un fuerte compromiso con la educación y la cooperación.

¿Mi consejo? Manténgase alerta, acepte el cambio, aprenda constantemente de la comunidad y no olvide retribuir. De esta manera, podemos garantizar un futuro más seguro para todos.

David Morimanno



**Director de Tecnologías de Gestión de Identidades y Accesos,
Integral Partners, una empresa de Xalient**

Los hallazgos del Informe de Vulnerabilidades de Microsoft de este año confirman lo que hemos visto en el panorama contemporáneo de la ciberseguridad. A medida que los ciberdelincuentes aumentan su enfoque en las vulnerabilidades centradas en las identidades, un programa sólido de gestión de accesos e identidades desempeña un papel fundamental para mitigar las amenazas en evolución. Esto es particularmente cierto para las amenazas centradas en vulnerabilidades de identidades dentro del ecosistema de Microsoft, facilitadas por la expansión de plataformas en la nube como Azure y Microsoft 365. Los sistemas complejos e interconectados introducen vulnerabilidades imprevistas, lo que requiere un enfoque proactivo para las medidas de seguridad centradas en la identidad.

La implementación de principios de Zero Trust se ha convertido en un enfoque clave para muchas de las organizaciones con las que trabajamos, al igual que la construcción de una estructura de identidades, que ofrece las capacidades necesarias para proporcionar un acceso fluido y controlado para todos a cada servicio. Integrar la gestión de accesos privilegiados en esta estructura de identidades más amplia es imperativo para fortalecer las medidas de seguridad y evitar posibles ataques cibernéticos.

¿Por qué el número de vulnerabilidades notificadas se ha mantenido estable?

En este informe, el número de vulnerabilidades de Microsoft se ha mantenido relativamente estable. ¿Porqué? Los esfuerzos de la empresa para parchear rápidamente las vulnerabilidades conocidas pueden estar compensando el descubrimiento de otras nuevas al reducir la ventana de oportunidad para que los atacantes exploten las vulnerabilidades. Además, a medida que el código base de MS madura, es posible que se introduzcan nuevas vulnerabilidades a un ritmo más lento. Otra posibilidad es que los productos de Microsoft a menudo dependan de bibliotecas y componentes de terceros, lo que podría introducir vulnerabilidades que no son directamente atribuibles al código de Microsoft.

La importancia de PAM y su contribución a la estructura de identidades

El incidente CVE-2023-23397 subraya los peligros de la dependencia de contraseñas y los controles de acceso inadecuados. ¡El exploit sin clic no requirió interacción del usuario, lo que permitió que un sistema vulnerable se viera comprometido a través de un email no abierto! Estos ataques enfatizan la necesidad de autenticación multifactor (MFA), segmentación, privilegios mínimos y parches oportunos para mitigar riesgos similares. Obviamente, PAM desempeña un papel crucial en la mitigación como parte de un programa holístico centrado en las identidades que fortalece su estructura de identidades más amplia, que abarca IGA, gestión de accesos, servicios de directorio y gestión de derechos de infraestructura en la nube (CIEM).

Una de las muchas herramientas que utilizamos en nuestra práctica de asesoramiento para ayudar a las organizaciones a abordar eficazmente los riesgos relacionados con las identidades es un checklist de evaluación de riesgos de identidades, que abarca facetas como la gobernanza, la gestión del ciclo de vida, los accesos privilegiados y las identidades de las máquinas.

También enfatizamos la necesidad de aprovechar la inteligencia artificial (IA) siempre que sea posible. Sin duda, el futuro de la seguridad centrada en las identidades aprovechará tecnologías avanzadas como la inteligencia artificial y el análisis del comportamiento para detectar y responder a las amenazas en tiempo real, garantizando que las organizaciones sigan siendo resilientes frente a los riesgos cibernéticos en constante evolución.

Greg van der Gaast



Director General
Sequoia Consulting

sequoia-consulting.co.uk

greg@sequoia-consulting.co.uk

Greg van der Gaast es director general de Sequoia Consulting, una asesoría de seguridad especializada que se enfoca en abordar problemas del negocio y de procesos para que haya menos incidentes de seguridad.

“El valor de las vulnerabilidades”

Pensé que podría contribuir con consejos prácticos sobre cómo aprovechar sus vulnerabilidades de manera más estratégica y analizar cosas más importantes que una calificación CVSS.

Si queremos avanzar en la mejora de la postura de seguridad de nuestra organización, en lugar de apagar incendios, debemos preocuparnos menos de las vulnerabilidades que tenemos y más de por qué las tenemos.

Por ejemplo, tener el CVE hipotético de puntuación CVSS 9.8 que salió recientemente no me preocupa. Mi proceso de aplicación de parches debería gestionarlo en un plazo de 24 a 48 horas.

Si este no es tu caso, te sugiero que dediques más tiempo a madurar tu programa de parches. Si hay razones por las que no podemos parchear, deberíamos preguntarnos por qué ellas existen, si son estrictamente necesarias y qué podemos hacer para cambiar eso.

Los CVE más recientes, mejores, grandes y aterradores no me preocupan. Lo que me preocupa es la vulnerabilidad de “bajo riesgo” de dos años. Su presencia me está diciendo algo.

Si ha estado ahí todo el tiempo, entonces es posible que haya algún problema grave con mi parche operativo.

Si acaba de aparecer, ¿tengo algún problema con la forma en que se construyen los nuevos sistemas? ¿O cómo es posible instalar software antiguo y vulnerable en sistemas existentes? Tal vez esos procesos estén bien, pero ¿hay un problema de adquisiciones o de TI en la sombra que los evita?

Son estos problemas en nuestros procesos los que crean la acumulación de riesgos que contribuirán a una eventual infracción. Abordarlos genera reducciones acumulativas y sostenibles en la cantidad de riesgo que presenta el negocio a lo largo del tiempo, lo que significa que cada vez tenemos menos de qué preocuparnos.

Encontrar estos problemas puede ser sorprendentemente fácil: las vulnerabilidades nos dicen exactamente dónde están estos problemas.

Las vulnerabilidades que hemos solucionado en el pasado, sin considerar de dónde vinieron, pueden haber sido un oportunidad perdida de encontrar la causa raíz de lo que nos hará vulnerar en el futuro.

Terry Cutler



**Hacker Ético y Fundador,
Cyology Labs**

Proteger su negocio: consejos de un hacker profesional

La realidad es que, ya sea que opere como un empresario en solitario o administre una empresa próspera, es esencial reconocer la ciberseguridad. Las amenazas pueden apuntar a cualquiera. A medida que las ciberamenazas evolucionan en complejidad, ninguna entidad permanece inmune. Las tendencias recientes revelan un aumento significativo en los incidentes que afectan a los gobiernos locales, los municipios y las empresas, y que resultan en pérdidas financieras sustanciales.

Cómo operan los piratas informáticos: el manual del experto

Los piratas informáticos suelen emplear un enfoque de ataque estructurado que implica consistentemente algunas fases. Comienzan con el reconocimiento, recopilando información digital, similar a rastrear rutas de navegación. Luego, realizan escaneos para encontrar vulnerabilidades, como un ladrón que busca puertas abiertas.

Una vez que encuentran un punto de entrada, continúan explotándolo para obtener y mantener el acceso, mientras cubren sus huellas. Finalmente, perturban sistemáticamente los sistemas.

El plan de juego para la resiliencia cibernética

La implementación de prácticas básicas de ciberseguridad puede prevenir muchos ataques. Acciones simples, como mantener actualizado su software, estar al día con los parches emitidos por Microsoft, tener cuidado con las estafas de phishing y usar contraseñas únicas y seguras con verificación en dos pasos son esenciales, como el Informe de BeyondTrust ha demostrado que eliminar derechos de administrador innecesarios y lograr privilegios mínimos es un paso vital en este proceso. Es como cerrar puertas y ventanas con llave: simple, pero eficaz para mantener alejados a los intrusos y permitir el acceso solo a la persona adecuada en el momento adecuado.

Llevar a cabo una investigación cibernética integral. La evaluación para descubrir cualquier vulnerabilidad es crucial

Para proteger su red, endpoints e infraestructura de nube de manera efectiva, adopte estrategias avanzadas como autenticación multifactor (MFA), cifrado, identidades y accesos, además de modernas de ciberdefensa. Personalice sus defensas según sus riesgos específicos y prepárese para adaptarse para mantenerse al día con las amenazas en evolución.

Sami Lai Ho



MVP del sistema operativo Windows
Chief Research Officer / Founder, Adminize

[LinkedIn](#)
[X \(anteriormente Twitter\)](#)

Como dice el Informe, "las vulnerabilidades totales continúan su patrón de retención de 3 años cerca de los números más altos de la historia." Dejamos de testar las actualizaciones de definiciones de antimalware antes de implementarlas porque ahora hay actualizaciones mensuales de Windows. ¿A veces fallaron? Sí. ¿Dejamos de actualizar? No. Creo que cualquiera de nosotros elegirá un posible tiempo de inactividad de dos horas para el cual estemos preparados y que tengamos bajo control, en lugar de un tiempo de inactividad de tres meses controlado por un tercero.

Tengo una regla con mis clientes: los parches críticos o los parches para cualquier cosa con una IP pública se parchearán los días 1-3. Todo lo demás se parchea lo antes posible, y para sus firewalls y gateways de VPN, usted aplica parches todos los días que comienzan con la letra T: Tuesday, Thrusday, Today y Tomorrow. Con el principio de privilegio mínimo, aún podemos mitigar alrededor de la mitad de todas las vulnerabilidades críticas, por lo que sigue siendo una de las leyes inmutables de la seguridad de Windows; como dice la guía del usuario de NT 3.1 de 1993, no hay seguridad en Windows si inicias sesión como administrador.

Afortunadamente, Zero Trust (por muy mal nombre que sea) ha puesto en boca de la mayoría de nosotros el Principio del Mínimo Privilegio. Los actores maliciosos necesitan derechos de administrador para ejecutar herramientas realmente peligrosas, y eso es lo que buscan. Como muestra el Informe, "La elevación de privilegios representó el 40% (490) del total de vulnerabilidades en 2023."

"Dado que los privilegios son lo que los actores de amenazas quieren, nuestro trabajo debe ser asegurarnos de que no los obtengan."

**Sami Laiho, MVP Del Sistema Operativo Windows,
Chief Research Officer/CEO, Truesec Finland**

Eliza May Austin



CEO
th4ts3cur1ty.company

Gestión de vulnerabilidades, elevación de privilegios e identidades como superficie de ataque

Vemos en los resultados de este informe que la fase de elevación de privilegios (PrivEsc) continúa siendo una táctica ofensiva exitosa. PrivEsc, una fase de ataque necesaria y requerida, se convertirá en el foco de los actores de amenazas, incluso más que penetrar el perímetro.

La previsibilidad de un perímetro estructurado en el sentido clásico está disminuyendo, con empresas de todos los tamaños apuntando a reducir sus arquitecturas clásicas en favor del enfoque "sin servidor". La identidad del usuario se convertirá en la superficie de ataque preferida, frente al perímetro tradicional. Los actores de amenazas atacarán las identidades (la cuenta) en lugar de comprometer el sistema, a medida que las empresas se alineen más con el concepto Zero Trust. Esto significa que, en teoría, se puede eludir el Zero Trust.

La concentración en el titular de la cuenta conducirá a un aumento en la necesidad de estructuras y capacidades de análisis forense digital y respuesta a incidentes (DFIR). Es crucial reconocer la gran cantidad de datos recopilados por los adversarios. Esto podría compararse con datos corporativos con información personal, lo que permitiría a los adversarios identificar vulnerabilidades específicas en el titular de la cuenta. Esto, a su vez, facilita ataques muy selectivos contra las identidades de las personas. Estos ataques pueden explotar eficazmente las debilidades del titular de la cuenta para obtener acceso donde de otro modo se habría requerido un ataque de día cero. Cuesta tiempo, dinero y recursos humanos desarrollar ataques personalizados nunca antes vistos (días cero), y si un grupo de amenazas puede evitar quemar uno (usarlo) centrándose en las identidades, entonces lo harán. Siempre buscarán lo más fácil y atacarán a los usuarios que cometan errores o a los sistemas que no estén bien defendidos.

El comentario de Eliza-May continúa en la página siguiente >

Sin duda, atacar cuentas conducirá a ataques a la cadena de suministro más complejos y, francamente, impresionantes. Incluso es posible que veamos que esto se expanda aún más, con ataques evolucionando hacia formas de más distanciadas, de proveedor-proveedor a proveedor-objetivo, y así sucesivamente. A medida que la dependencia de SaaS continúa creciendo en un intento de eludir esta expansión, notaremos un aumento en lo que me gusta llamar 'Jackpotattacks', como los de SolarWinds y FireEye.

Volviendo al Informe de vulnerabilidades de Microsoft, es crucial priorizar la gestión de vulnerabilidades y educar a las empresas sobre cómo distinguir entre scanning y gestión. Adquirir licencias de scanning es simple, pero establecer un proceso interno para identificar, priorizar, remediar y probar mitigaciones sigue siendo un desafío constante, debido a las dependencias entre departamentos y la falta de KPI que midan la reducción de la exposición a las vulnerabilidades.

Marc Maiffret



CTO
BeyondTrust

Como CTO de BeyondTrust y fanático de Spinal Tap, estoy entusiasmado de ver que este informe **está en su 11a edición**. Además de ser "uno más que diez" (lo prometo, no más referencias a Spinal Tap), el informe continúa destacando la necesidad de seguir mejorando la seguridad, no solo en Microsoft, sino también para todas las organizaciones que buscan gestionar mejor la seguridad cibernética y los riesgos en el contexto de un panorama de amenazas en evolución.

Si bien el número de vulnerabilidades críticas de Microsoft está alcanzando mínimos históricos, hay algunos buenos ejemplos en el informe de razones para no hacerlo y volverse complaciente cuando se trata de vulnerabilidades. A pesar de los grandes avances en la seguridad general del ecosistema de Microsoft, CVE-2023-23397 permitiendo capturar hashes NTLM a través de Outlook y CVE-2023-36884 permitiendo omitir Mark of the Web, ambos nos muestran que todavía hay muchas superficies de ataque que esperan ser encontradas y explotadas.

El dominio continuo de la elevación de privilegios como la categoría más común de vulnerabilidades y la crisis de identidades resaltada al final de el informe, destacan la importancia del privilegio y el concepto de seguridad atemporal del privilegio mínimo.

El comentario de Marc continúa en la página siguiente >



Al principio de mi carrera, tuve la suerte de conocer los Rainbow Books, una serie de estándares de seguridad informática publicados por el Departamento de Defensa americano en las décadas de 1980 y 1990. Estos libros, y los conceptos de superficie de ataque y privilegio mínimo que se describen en ellos, son tan relevantes para los desafíos que enfrentamos hoy como lo fueron hace más de 30 años, cuando los libros se publicaron por primera vez.

"Mínimo privilegio: este principio requiere que a cada sujeto de un sistema se le otorgue el conjunto más restrictivo de privilegios necesarios para la realización de tareas autorizadas. La aplicación de este principio limita el daño que puede resultar de un accidente, error o uso no autorizado."

**A Guide To Understanding Discretionary Access Control
In Trusted Systems, 1987**

Cuando pienso en la seguridad de las identidades hoy en día, no son las identidades en sí las que tienen valor, son los privilegios a los que esas identidades pueden acceder los que tienen valor y las convierten en un objetivo. Esta es la razón por la que los actores de amenazas buscan vulnerabilidades de elevación de privilegios e identidades con acceso a privilegios. Es por eso que los parches y los privilegios mínimos siguen siendo algunas de las mejores formas de reducir la superficie de ataque. También es la razón por la que BeyondTrust tiene la misión de brindar el más amplio nivel de visibilidad y protección de privilegios.

El ataque de Midnight Blizzard al que se hace referencia en el informe de este año fue una excelente ilustración del panorama moderno de amenazas a las identidades. Con eso en mente, voy a lanzar un desafío a los autores de este informe para el próximo año para que vayan más allá de las vulnerabilidades del software de Microsoft y analicen algunas de las configuraciones erróneas comunes o configuraciones predeterminadas débiles que introducen vulnerabilidades de configuración en el ecosistema de Microsoft, permitiendo atacantes para acceder a privilegios y explotar sistemas.

¡Manténgase a salvo!

Dra. Jessica Barker MBE



Cofundador de Cygenta

Autora de Hacked: The Secrets Behind Cyber Attacks

[LinkedIn](#)

[X \(Twitter\)](#)

Los datos de este año siguen mostrando que trabajar en seguridad vale la pena.

Al trabajar en esta industria, a veces podemos sentir que no avanzamos, o incluso que estamos retrocediendo; que los atacantes ganan mucho más a menudo que nosotros.

Tenemos que buscar los defectos: la única vez que algo sale mal en lugar de las 100 veces que sale bien. Y con un panorama de amenazas en constante evolución, podemos sentir que nadamos contra corriente.

Es por eso que debemos mirar el panorama más amplio, reconociendo que los complejos problemas de ciberseguridad no se resolverán de la noche a la mañana y logramos muchos avances a lo largo del camino.

No sorprende que la escalada de privilegios siga siendo la categoría número uno de vulnerabilidad en el informe de este año. Pero incluso esta, la categoría número uno de vulnerabilidad, muestra una marcada mejora. Esto sirve como recordatorio de que no podemos arreglar todo de la noche a la mañana, pero podemos avanzar, incluso en áreas difíciles.

El informe de este año destaca que los atacantes "piensan en gráficos". En ciberseguridad, también debemos pensar en los sistemas. Cuando se trata de ingeniería social y el lado humano de la seguridad, puede resultar fácil centrarse en el llamado error humano. Sin embargo, si nos centramos únicamente en el individuo, no damos en el blanco.

En lugar de ello, debemos observar los sistemas en los que operan las personas, reduciendo la carga para los usuarios finales. Las redes segmentadas, los privilegios mínimos, la autenticación multifactor y la gestión de vulnerabilidades son fundamentales y están respaldados por una cultura de seguridad saludable.

Este informe también destaca la importancia de la identidad. Con el auge de la IA generativa y la tecnología deepfake utilizada en ataques de ingeniería social, la gestión de identidades se convertirá en un problema aún más apremiante. Es más crucial que nunca que generemos conciencia sobre las amenazas y, al mismo tiempo, hagamos todo lo posible para reducir las fricciones en materia de seguridad, capacitando a las personas para que practiquen comportamientos seguros dentro de una cultura de seguridad positiva y proactiva.



Mitigando los Riesgos del Ecosistema de Microsoft y Mejorando la Resiliencia Cibernética

Juntas, las siguientes estrategias de seguridad brindan una protección altamente efectiva contra vulnerabilidades de Microsoft y también ataques basados en identidades:

- 1. Implemente el privilegio mínimo eliminando los derechos de administrador local:** Es esencial mantener una estrategia sólida de gestión de accesos privilegiados para eliminar y proteger los privilegios dentro de un entorno para evitar que caigan en manos de un atacante. Este enfoque proactivo puede proporcionar una protección muy eficaz, incluso en ausencia de parches. Históricamente, eliminar los derechos de administrador local y controlar la ejecución ha mitigado el 75% de las vulnerabilidades críticas de Microsoft, como hemos demostrado en informes anteriores cuando Microsoft puso a disposición más datos específicos de privilegios. Esta estadística del 75% indica que, sin derechos de administrador, la vulnerabilidad no se puede explotar, incluso si no se ha parcheado. Un enfoque de privilegios mínimos, que también es un principio fundamental de los modelos de seguridad de Zero Trust, puede ayudar a romper múltiples puntos en la cadena de ataque, desde el secuestro de cuentas hasta el movimiento lateral, pasando por la escalada de privilegios y más.
- 2. Siga los protocolos de refuerzo de seguridad, como la aplicación de parches:** Asegúrese siempre de que su sistema operativo y el software de terceros estén actualizados y no está utilizando software al final de su vida útil en su entorno. Además, elimine privilegios, accesos y cuentas innecesarios para reducir aún más la superficie de riesgo. Tenga en cuenta que aplicar parches lo antes posible también puede ayudarle a evitar que una vulnerabilidad aparentemente inofensiva se convierta en una amenaza mayor.
- 3. Vías seguras de acceso remoto:** El Remote Desktop Protocol (RDP) de Microsoft, así como las VPN y muchas otras tecnologías comunes de acceso remoto, se extienden cada vez más allá de sus casos de uso adecuados, lo que genera exposiciones de seguridad y violaciones. El ransomware suele utilizar RDP como punto de entrada. Asegúrese de que RDP no esté expuesto a Internet. No permita que se mezclen VPN y BYOD. Reemplace las VPN o aumentelas con controles de seguridad de Zero Trust para casos de uso de accesos de proveedores y privilegiados.
- 4. Adapte la gestión de vulnerabilidades a su propio entorno:** Es fundamental encontrar, priorizar y determinar una ruta de solución para todas las vulnerabilidades. Sin el contexto de los modelos de amenazas de su propia organización, no puede comprender completamente cuál es la mejor manera de priorizar los parches y/o utilizar otros controles y mitigaciones para reforzar la seguridad. Lo que se considera un parche crítico para una organización puede no serlo para otra. Aproveche su contexto empresarial para crear la estrategia de gestión de vulnerabilidades que mejor aborde sus riesgos.
- 5. Esté atento a las amenazas emergentes:** Comprender las amenazas contribuye en gran medida a tomar decisiones más informadas y a mantenerse seguro. La última década ha marcado el comienzo de cambios considerables en el panorama de amenazas de Microsoft. Con el rápido desarrollo e implementación de tecnologías de IA, es probable que veamos muchos cambios impactantes en las amenazas durante la próxima década y más allá.
- 6. Implementar Detección y Respuesta a Amenazas de Identidad (ITDR):** Las organizaciones deben realizar cambios y correcciones proactivas en la postura de seguridad para evitar que las amenazas se afiancen, y también deben organizar una respuesta rápida a cualquier ataque que asoma la cabeza. ITDR, o esencialmente defensa en profundidad de las identidades es un enfoque multidisciplinario que tiene como objetivo integrar capacidades para la visibilidad integral de la seguridad de las identidades, la detección de amenazas, la investigación y las capacidades de respuesta. Esto comienza con una visibilidad completa de la postura de seguridad de las identidades en todos los almacenes (Active Directory, Entra ID, Okta, Ping y más). A partir de ahí, las organizaciones pueden comprender las rutas de ataque que pueden operar a través de esas identidades y qué pasos se necesitan para mejorar la postura o detener un ataque.



Cómo BeyondTrust Mitiga las Vulnerabilidades Tradicionales y los Riesgos Modernos Basados en las Identidades

BeyondTrust combina una gestión completa de los accesos privilegiados, con capacidades CIEM e ITDR, para mitigar las vulnerabilidades de Microsoft y proteger toda la infraestructura de identidades, desde Active Directory hasta Entra ID y más.

Los clientes confían en las soluciones de BeyondTrust para:

- Eliminar derechos de administrador e implementar un verdadero modelo de privilegios mínimos coherente con los principios de Zero Trust.
- Asegurar la infraestructura y las vías de acceso remoto, garantizando que todo el acceso de los empleados, proveedores y otras personas sea granular, controlado y auditado.
- Evitar el secuestro de cuentas y la escalada de privilegios mediante la gestión segura de todas las credenciales privilegiadas de humanos y máquinas,. Secretos de DevOps, claves SSH y contraseñas de la fuerza laboral de los empleados que afectan a la empresa.
- Administrar, monitorear y auditar cada sesión privilegiada, sin importar cuán efímera sea.
- Administrar y reducir de manera efectiva toda la superficie de ataque de identidades, que abarca Microsoft y otros almacenes de identidades (Okta, Ping, etc.).
- Detectar y neutralizar ataques de identidades con velocidad y precisión.
- Satisfacer rigurosos requisitos forenses y de cumplimiento proporcionando fácil acceso a informes sobre todas las actividades privilegiadas y otros conocimientos de identidades.
- Calificar para un seguro cibernético reuniéndose con varios controles de seguridad clave exigidos por los proveedores de seguros cibernéticos y los suscriptores de pólizas.

Con BeyondTrust, las organizaciones obtienen lo mejor de ambos mundos: la protección proactiva contra amenazas externas (ransomware), malware, etc.) y amenazas internas, con capacidades de detección y respuesta para detener ataques en curso. [Más información.](#)

"Las credenciales privilegiadas de larga duración aparecen en muchos informes de infracciones. Tenemos que gestionarlas mejor y eliminarlas donde podamos".

Jay Beale, CEO, CTO InGuardians, Inc

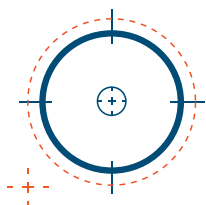
Conclusión

Si bien el total de vulnerabilidades de Microsoft se mantiene ligeramente por debajo de sus máximos históricos, se han estancado más o menos desde 2020. Durante este mismo período, el número de vulnerabilidades críticas ha continuado su tendencia a la baja.

La estabilización en el número total de vulnerabilidades refleja las importantes inversiones en seguridad y el enfoque por parte de Microsoft. Sin embargo, como lo han demostrado algunas vulnerabilidades críticas sorprendentes y nuevas tácticas de amenaza innovadoras aprovechadas el año pasado, ahora no es el momento de volverse complacientes. Existen numerosas vulnerabilidades para todos, incluidos sistemas sin parches con vulnerabilidades conocidas que hacen que sea muy fácil para los actores de amenazas lanzar un ataque exitoso.

Además, como el patrimonio tecnológico de Microsoft continúa expandiéndose, traerá consigo nuevas superficies de ataque y vectores de amenazas potenciales. Las vulnerabilidades también seguirán surgiendo de maneras nunca antes vistas, y los actores de amenazas seguirán pensando en gráficos para navegar por caminos innovadores a través de los sistemas de Microsoft.

Como hemos demostrado en los 11 años que lleva publicándose este informe, el panorama de vulnerabilidades de Microsoft está en constante evolución. Si bien las vulnerabilidades siguen siendo una parte importante de la superficie de ataque, las inversiones en investigación y prácticas de seguridad obligan cada vez más a los actores de amenazas a innovar. Esto seguirá cambiando la forma en que los actores de amenazas se afianzan en los entornos de las víctimas.



Estamos alcanzando rápidamente un punto de inflexión notable en el que cada vez es más fácil para los actores de amenazas robar una identidad para obtener acceso que explotar una vulnerabilidad.

Esto significa que podemos esperar que el volumen y la sofisticación de los ataques basados en identidades aumenten considerablemente a medida que los actores de amenazas se centren en las identidades como un medio de ataque mucho más fructífero.

Una noticia favorable para los defensores es que los principios de seguridad fundamentales y de larga data que se han probado durante la última década continúan ofreciendo la mejor línea de defensa, incluso contra las amenazas modernas.

Un mínimo de privilegios es fundamental para reducir todas las superficies de ataque en todos los endpoints e identidades. Cuantos menos privilegios tenga la víctima, menor será el riesgo de que la cuenta se vea comprometida, incluso durante ataques de día cero, e incluso cuando un atacante aplica ingeniería inversa a un parche para encontrar una solución alternativa explotable.

Aquellas organizaciones que combinen con éxito controles de seguridad preventivos con detección y respuesta a amenazas seguirán estando mucho mejor preparadas para resistir las amenazas del futuro. Y, como siempre, continuaremos ofreciendo nuestros conocimientos para ayudar a nuestros lectores a mantenerse alerta sobre las últimas amenazas, las vulnerabilidades más impactantes y las estrategias más efectivas para fortalecer su postura de seguridad.

Metodología

El segundo martes de cada mes (conocido como "Patch Tuesday"), Microsoft publica boletines de seguridad que anuncian correcciones para cualquier vulnerabilidad que afecte a sus productos.

El Informe anual de vulnerabilidades de Microsoft de BeyondTrust recopila estas versiones en una descripción general de un año y analiza los datos, creando una visión holística de las tendencias relacionadas con las vulnerabilidades.

Hasta noviembre de 2020, Microsoft había estado utilizando su propio método para compartir detalles de CVE a través de su Guía de actualización de seguridad.

El antiguo formato de informes de Microsoft solía traer un resumen ejecutivo para cada vulnerabilidad reportada que incluiría la siguiente palabrería:

- Los clientes/usuarios cuyas cuentas están configuradas para tener menos derechos de usuario en el sistema podrían verse menos afectados que los usuarios que operan con derechos de usuario administrativos.
- Si el usuario actual inicia sesión con derechos de usuario administrativo, un atacante podría tomar el control de un sistema afectado.

A partir de este resumen, los investigadores pudieron deducir si alguna vulnerabilidad determinada (específicamente, las críticas) podría haberse mitigado si se hubieran eliminado los derechos de administrador del usuario.

En 2021, Microsoft cambió de metodología y pasó a el Sistema Común de Puntuación de Vulnerabilidad (CVSS). Y en 2023, continuó usando la puntuación CVSS 3.1 para sus vulnerabilidades, pero comenzó a clasificar la gravedad según su propio sistema de clasificación de gravedad de actualizaciones de seguridad.

La metodología CVSS permite comparar más fácilmente las vulnerabilidades de Microsoft con errores de terceros, lo que simplifica algunos análisis, y el sistema de clasificación de gravedad de las actualizaciones de seguridad permite clasificar cada vulnerabilidad según el peor resultado teórico, en caso de que se explote esa vulnerabilidad.

Sin embargo, una desventaja desafortunada de este cambio fue la pérdida de la capacidad de determinar el impacto de los derechos de administrador en las vulnerabilidades críticas.

No solo los riesgos del exceso de los accesos privilegiados permanecen prácticamente intactos, sino que los vectores de ataque privilegiados están creciendo rápidamente con la expansión de la nube y la proliferación de identidades y cuentas humanas y de máquinas.

Por lo tanto, si bien las estadísticas sobre derechos de administrador pueden estar ausentes en el informe de este año, es imperativo que las organizaciones no se vuelvan complacientes. La eliminación de los derechos de administrador sigue siendo una pieza clave de una estrategia de privilegios mínimos, así como para permitir el Zero Trust.



Precisión de los Datos de Vulnerabilidad

Se han realizado una serie de generalizaciones para cada vulnerabilidad, de la siguiente manera:

- Cada vulnerabilidad se clasificó de acuerdo con la gravedad más alta de todas las instancias de esa vulnerabilidad donde apareció varias veces.
- Cada vulnerabilidad se clasificó con el tipo más frecuente para todas las instancias de esa vulnerabilidad.
- No se tuvieron en cuenta las versiones del producto.
- No se tuvieron en cuenta las combinaciones de productos.
- Se contaron las vulnerabilidades tanto para el software como para la versión cuando correspondía (por ejemplo, una vulnerabilidad para Microsoft Edge en Windows 10 se toma como una vulnerabilidad tanto para Edge y Windows)

>>> Recursos adicionales

EVALUACIÓN	<u>Gain Control Over Your Entire Identity Attacks Surface:</u> Comience con una evaluación gratuita de la seguridad de las identidades y un monitoreo de su patrimonio de TI para detectar privilegios excesivos, configuraciones incorrectas (falta de MFA, etc.) cuentas huérfanas, ataques en curso y mucho más. Obtenga también información clara sobre el contexto de las amenazas y los pasos para remediarlas.
TESTE/CHECKLIST	<u>Need a VPN Alternative?</u> Realice la prueba de acceso remoto: descubra si su equipo cuenta con las herramientas de acceso remoto seguras adecuadas para manejar el gran volumen de usuarios que se conectan de forma remota a su red.
CHECKLIST	<u>Cybersecurity Insurance Checklist:</u> Aproveche nuestra lista de verificación para ver qué tan bien su organización cumple con los estrictos requisitos de suscripción necesarios para calificar para el seguro cibernético.
GUÍA DE SOLUCIONES	<u>A Guide to Endpoint Privilege Management:</u> Descubra cómo la administración de privilegios de endpoints (EPM) combina privilegios mínimos con el control de aplicaciones para reducir significativamente la superficie de ataque en Windows, macOS y Linux.
WHITE PAPER	<u>Buyer's Guide for Complete Privileged Access Management (PAM):</u> Comprenda las capacidades PAM imprescindibles y necesarias para proteger adecuadamente las identidades y el acceso en todo su entorno, eliminar y mitigar muchos vectores de amenazas y ayudarle a avanzar en su recorrido PAM.
BLOG	<u>Shelter from the Storm – What Midnight Blizzard's Attack on Microsoft Tells Us about Modern Identity-Based Attacks:</u> lo que nos dice el ataque de Midnight Blizzard a Microsoft sobre los ataques modernos basados en identidad: Descubra las características únicas que distinguen a este ataque y descubra por qué este ataque de estado-nación contra Microsoft destaca la importancia de un enfoque de seguridad que priorice la identidad.

>>> Acerca de BeyondTrust

BeyondTrust es el líder mundial en ciberseguridad que protege todos los caminos hacia el privilegio. Nuestro enfoque centrado en las identidades va más allá de la protección de los privilegios y de los accesos, ya que permite a las organizaciones disponer de la solución más eficaz para gestionar toda la superficie de ataque a las identidades y neutralizar las amenazas, ya sean de ataques externos o internos.

BeyondTrust lidera la transformación de la seguridad de las identidades para prevenir brechas y limitar el radio de explosión de los ataques, al tiempo que crea una experiencia de cliente superior y eficiencias operativas. Contamos con la confianza de 20.000 clientes, incluidos 75 de la lista Fortune 100, y de nuestro ecosistema global de socios.

Conozca más en www.beyondtrust.com/es.