Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

MICROSOFT LANZA PARCHES CRÍTICOS EN ‘PATCH TUESDAY’ DE MARZO 2024

13 / 03 / 2024

CONTENIDO

INTRODUCCIÓN

En su última actualización mensual de seguridad conocida como "Patch Tuesday", Microsoft ha lanzado correcciones para dos vulnerabilidades críticas, junto con un total de 61 parches nuevos. A pesar de abordar un amplio espectro de productos de Microsoft, incluyendo Windows, Office, Azure y Visual Studio, este lanzamiento se destaca por su volumen relativamente bajo en comparación con meses anteriores. Además, se señala la ausencia de explotaciones conocidas hasta el momento para las vulnerabilidades corregidas.

MICROSOFT LANZA PARCHES CRÍTICOS EN ‘PATCH TUESDAY’ DE MARZO 2024

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_03_13_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	13/03/2024
Es día cero (0 day):	No

RESUMEN

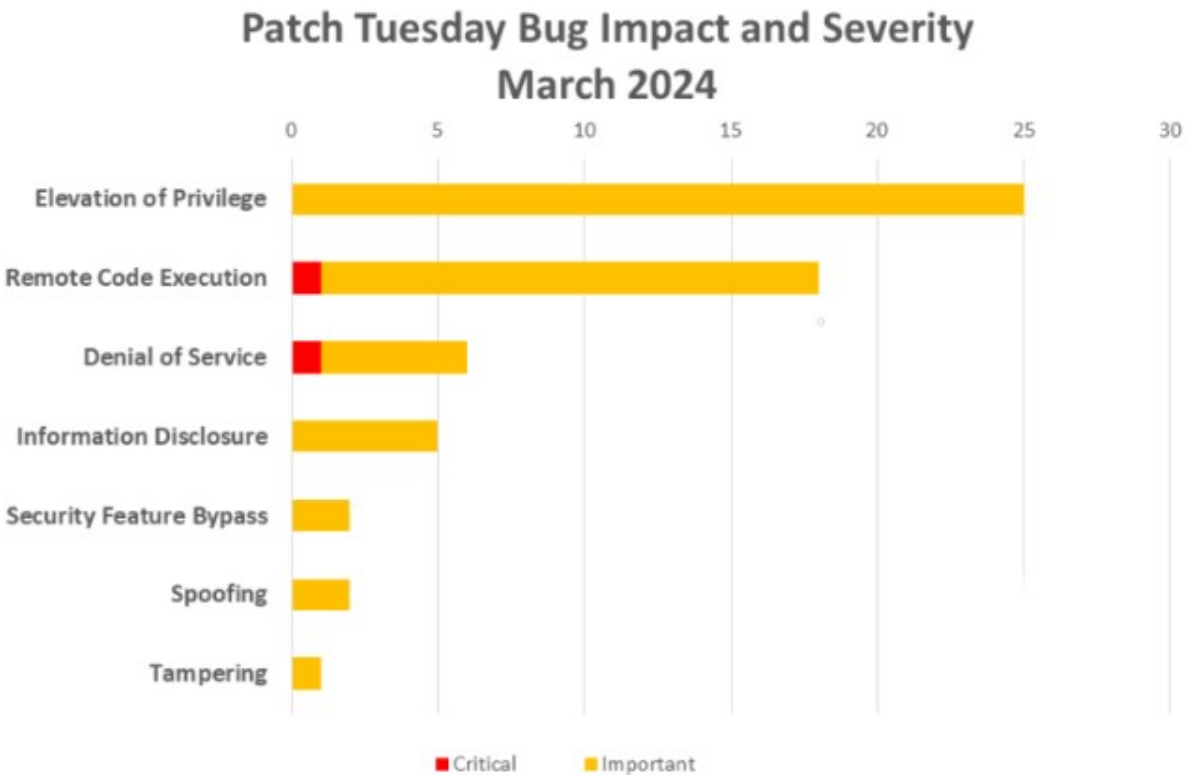
Microsoft ha lanzado su actualización de seguridad de marzo 2024, abordando un total de 61 vulnerabilidades. Dos de estas vulnerabilidades se clasifican como críticas en las advertencias de Microsoft, destacando la importancia de aplicar estos parches de inmediato. Aunque no se han reportado vulnerabilidades de Zero-Day en esta actualización, es esencial tener en cuenta que el panorama de amenazas puede cambiar rápidamente.

Las fallas recibieron parches como parte de la actualización mensual de Microsoft, conocida popularmente como “Patch Tuesday”.

En esta ocasión, el parche se enfoca en diversas áreas críticas, con énfasis en:

- 18 vulnerabilidades de Ejecución Remota de Código (RCE)
- 24 vulnerabilidades de Elevación de Privilegios (EoP)
- 6 vulnerabilidades de Denegación de Servicio (DoS)
- 3Vulnerabilidades de Falsificación (Spoofing)
- 6 vulnerabilidades de Divulgación de Información
- 1 vulnerabilidad de Cross-site Scripting (XSS)
- 3 vulnerabilidades de Bypass de Funciones de Seguridad

Además, se ha identificado una “Vulnerabilidad de Manipulación de Carpetas Comprimidas” que afecta a Windows, aunque no se ajusta a las categorías de vulnerabilidad mencionadas anteriormente.



Entre las vulnerabilidades críticas abordadas, se destacan:

Vulnerabilidades RCE y DoS en Windows Hyper-V: CVE-2024-21407 y CVE-2024-21408

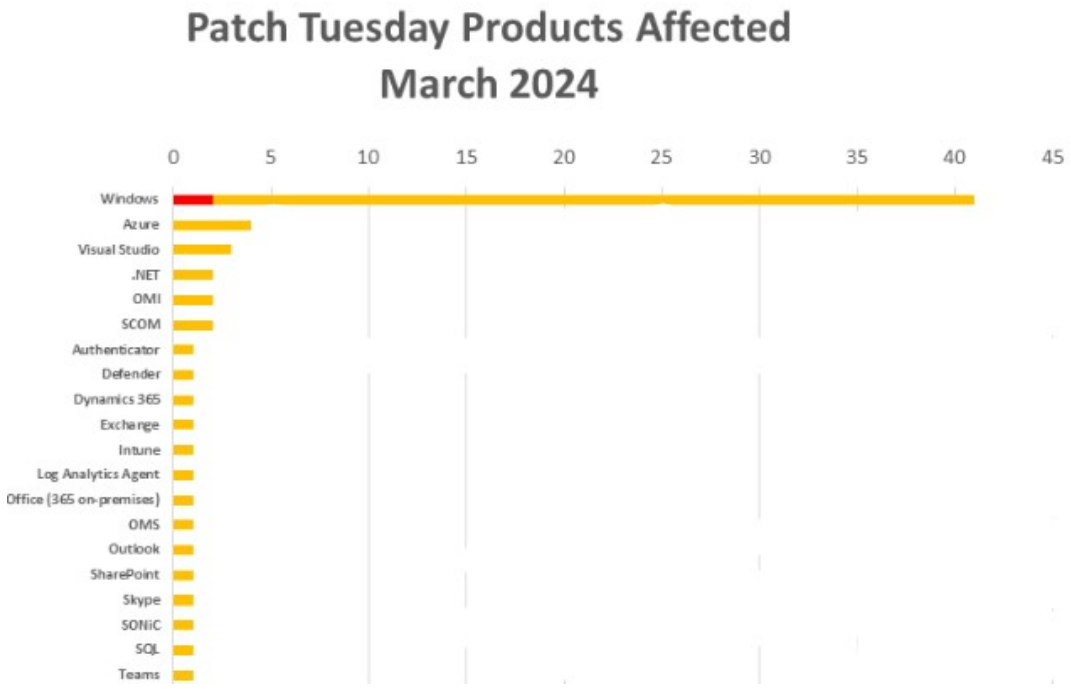
CVE-2024-21407: Una vulnerabilidad RCE con un puntaje de gravedad de 8.1, que podría permitir a un atacante autenticado en una máquina virtual (VM) enviar solicitudes de operaciones de archivos especialmente diseñadas para ejecutar código en el servidor host.

CVE-2024-21408: Aunque menos grave con un puntaje de CVSS de 5.5, esta vulnerabilidad afecta la disponibilidad al causar una Denegación de Servicio (DoS) en Windows Hyper-V.

Vulnerabilidades Críticas Corregidas en Open Management Infrastructure y Azure Kubernetes Service: CVE-2024-21334 y CVE-2024-21400

CVE-2024-21334: Una vulnerabilidad RCE en Open Management Infrastructure con un puntaje CVSS de 9.8, que permite a un atacante remoto no autenticado aprovechar una vulnerabilidad de uso posterior a la liberación.

CVE-2024-21400: Una vulnerabilidad de Elevación de Privilegios en Azure Kubernetes Service con un puntaje CVSS de 9.0, que podría resultar en robo de credenciales y acceso no autorizado a nodos y contenedores.



En resumen, mientras que el lanzamiento de “Patch Tuesday” de marzo de 2024 no incluyó ninguna vulnerabilidad de Zero-Day o fallas explotadas activamente, es esencial que los usuarios apliquen los

parches necesarios de manera oportuna para mitigar los riesgos potenciales para sus sistemas y su infraestructura.

Varias vulnerabilidades de alta y mediana gravedad abordadas en esta actualización se consideran propensas a explotación y no cuentan con soluciones alternativas disponibles.

Es imperativo revisar estas vulnerabilidades y aplicar los parches correspondientes de manera inmediata para mitigar posibles amenazas de seguridad. Para obtener más detalles sobre las vulnerabilidades abordadas en la actualización de marzo 2024, consulte las notas de lanzamiento más recientes de Microsoft.

NOTICIA COMPLETA

https://devel.group/blog/microsoft-lanza-parches-criticos-en-patch-tuesday-de-marzo-2024/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente