Microsoft lanzó el martes sus actualizaciones de seguridad mensuales con correcciones para 51 vulnerabilidades en su línea de software que consta de Windows, Office, Teams, Azure Data Explorer, Visual Studio Code y otros componentes como Kernel y Win32k.

Entre las 51 vulnerabilidades corregidas, 50 están clasificadas como importantes y una tiene una clasificación de gravedad moderada, lo que la convierte en una de las raras actualizaciones de Patch Tuesday sin arreglos para las vulnerabilidades clasificadas como críticas. Esto también se suma a 19 fallas más que la compañía abordó en su navegador Edge basado en Chromium.

Ninguna de las vulnerabilidades de seguridad se enume

ran como explotación activa, mientras que las fallas CVE-2022-21989, con puntuación CVSS de 7.8, se clasificó como un día cero divulgado públicamente en el momento del lanzamiento. El problema se refiere a un error de escalada de privilegios en el kernel de Windows, y Microsoft advierte sobre posibles ataques que explotan la vulnerabilidad.

> *«La explotación exitosa de esta vulnerabilidad requiere que un atacante tome medidas adicionales antes de la explotación para preparar el entorno de destino. Se podría realizar un ataque exitoso desde un AppContainer con privilegios bajos. El atacante podría elevar sus privilegios y ejecutar código o acceder a recursos a un nivel de integridad más alto que el del entorno de ejecución de AppContainer»,* dijo la compañía en un aviso.

También se resolvieron una serie de vulnerabilidades de ejecución remota de código que afectan a Windows DNS Server (CVE-2022-21984, puntuación CVSS: 8.8), SharePoint Server (CVE-2022-22005, puntuación CVSS: 8.8), Windows Hyper-V (CVE-2022-21995, puntuación CVSS: 5.3) y extensiones de vídeo HEVC (CVE-2022-21844, CVE-2022-21926 y CVE-2022-21927, puntuaciones CVSS: 7.8).

La actualización de seguridad también corrigió una vulnerabilidad de suplantación de Azure

Data Explorer (CVE-2022-23256, puntuación CVSS: 8.1), dos vulnerabilidades de omisión de seguridad, cada una de las cuales afecta a Outlook para Mac (CVE-2022-23280, puntuación CVSS: 5.3) y OneDrive para Android (CVE-2022-23255, puntuación CVSS: 5.9) y dos vulnerabilidades de denegación de servicio en .NET (CVE-2022-21986, puntuación CVSS: 7.5) y Teams (CVE-2022-21965, puntuación CVSS: 7.5).

Microsoft también mencionó que corrigió múltiples vulnerabilidades de elevación de privilegios: cuatro en el servicio Print Spooler y una en el controlador Win32k (CVE-2022-21996, puntuación CVSS: 7.8), la última de las cuales ha sido etiquetada como *«Explotación más probable»* a la luz de una vulnerabilidad similar en el mismo componente que se corrigió el mes pasado (CVE-2022-21882) y que ha estado desde entonces bajo ataque activo.

Las actualizaciones llegan cuando la compañía volvió a publicar a fines del mes pasado una vulnerabilidad que data de 2013, un problema de validación de firma que afecta a WinVerifyTrust (CVE-2013-3900), y asegura que la solución *«está disponible como una función opcional a través de la configuración de clave de registro, y está disponible en las ediciones compatibles de Windows lanzadas desde el 10 de diciembre de 2013».*

El movimiento puede haber sido impulsado en respuesta a una campaña de malware ZLoader en curso que, como descubrió Check Point Research a inicios de enero, se descubrió que aprovechaba la vulnerabilidad para eludir el mecanismo de verificación de firmas de archivos y lanzar malware capaz de desviar las credenciales de los usuarios y otra información confidencial.

Parches de software de otros proveedores

Por otro lado, otros proveedores también lanzaron actualizaciones de seguridad para corregir varias vulnerabilidades, como:

- Adobe
- Android

- Cisco
- Citrix
- Google Chrome
- Intel
- Distribuciones de Linux Oracle Linux, Red Hat y SUSE
- Mozilla Firefox y Firefox ESR
- SAP
- Schneider Electric
- Siemens