Boletín de alerta

Boletín Nro.:
Fecha de publicación: 26/01/2026
Tema: Alerta 2026-09 Vulnerabilidad 0-day Office
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

• Microsoft Office 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft Office LTSC 2024, and Microsoft 365 Apps for Enterprise

Descripción

Es una vulnerabilidad de tipo 0-day que está siendo utilizada por atacantes en entornos de Microsoft Office. Etiquetado como CVE-2026-21509 con CVSSv3 7.8.

Este error depende de un elemento tan humano y habitual como lo es abrir un archivo. Los atacantes crean documentos de Office maliciosos y emplean métodos de ingeniería social para persuadir a las víctimas de ejecutarlos, con lo que logran eludir las defensas de seguridad locales que deberían impedir estas intrusiones por medio de controles internos del aplicativo.

El problema reside en la dependencia de datos no confiables en una decisión de seguridad en Microsoft Office permite a un atacante no autorizado eludir una función de seguridad localmente. Un atacante debe enviar a un usuario un archivo malicioso de Office y convencerlo de que lo abra. El panel de vista previa no supone un riesgo directo; sin embargo, el hecho de abrir un documento externo y confiar en él puede dar lugar a una explotación exitosa que comprometa la integridad del equipo de forma inmediata.

Solución

Los clientes de Office 2021 y versiones posteriores estarán protegidos automáticamente mediante un cambio en el servicio, pero deberán reiniciar sus aplicaciones de Office para que esto surta efecto.

Para Office 2016 y 2019 se requiere instalar los siguientes parches de seguridad:

- Microsoft Office 2019 (32-bit edition) – 16.0.10417.20095
- Microsoft Office 2019 (64-bit edition) – 16.0.10417.20095
- Microsoft Office 2016 (32-bit edition) – 16.0.5539.1001
- Microsoft Office 2016 (64-bit edition) – 16.0.5539.1001

Adicionalmente, Microsoft recomienda realizar un cambio en el Registro de Windows siguiendo los pasos que se describen a continuación:

- Realice una copia de seguridad del Registro.
- Cierre todas las aplicaciones de Microsoft Office.
- Inicie el Editor del Registro.
- Encuentre la subclave del Registro adecuada.
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\Common\COM Compatibility\ para MSI Office de 64 bits o MSI Office de 32 bits en Windows de 32 bits
    - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Common\COM Compatibility\ para MSI Office de 32 bits en Windows de 64 bits
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Mic Compatibility\ para Click2Run Office de 64 bits o Click2Run Office de 32 bits en Windows de 32 bits
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\WO Compatibility\ para Office Click2Run de 32 bits en Windows de 64 bits
- Agregue una nueva subclave denominada {EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B} haciendo clic derecho en el nodo Compatibilidad COM y seleccionando Agregar clave.
    - Dentro de esa subclave, agregue un nuevo valor haciendo clic derecho en ella y seleccionando «Nuevo > Valor DWORD (32 bits)».
    - Agregue un valor hexadecimal REG_DWORD llamado «Compatibility Flags» con un valor de 400.
- Salga del Editor del Registro e inicie la aplicación de Office

Información adicional:

- https://securityaffairs.com/187349/hacking/emergency-microsoft-update-fixes-in-the-wild-office-zero-day.html
- https://thecyberexpress.com/microsoft-emergency-fix-for-office-zero-day/
- https://www.neowin.net/news/microsoft-patches-serious-office-zero-day-vulnerability-already-being-exploited-in-attacks/