Incidente ID:	0027
Fecha del reporte:	27/01/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad en Microsoft Office
Herramienta de detección	N/A
Activo involucrado:	Microsoft
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alta

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la vulnerabilidad de zero-day CVE-2026-21509 que actualmente se encuentra siendo explotada activamente, esta vulnerabilidad afecta a varias versiones de Microsoft Office.

Esta vulnerabilidad es de nivel importante (CVSS: 7.8), esta es una vulnerabilidad de tipo Security Feature Bypass (omisión de funciones de seguridad). Debido a su facilidad de ser explotada y que actualmente ya está siendo explotada activamente por actores de amenaza, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) la agregó a su catálogo como vulnerabilidad que debe ser remediada lo más pronto posible.

Descripción:

El CVE-2026-21509 afecta varias versiones de Microsoft Office, es una vulnerabilidad de omisión de funciones de seguridad (Security Feature Bypass) en Microsoft Office. El fallo reside en la forma en que el software procesa entradas no confiables al tomar decisiones de seguridad, específicamente relacionadas con objetos OLE (Object Linking and Embedding).

La vulnerabilidad afecta a los controles OLE/COM que utiliza Office para ejecutar objetos externos. En un escenario ideal, un documento bloquea el uso de controles inseguros para

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

evitar riesgos. Con este fallo, el atacante solo requiere que se abra un documento de Microsoft Office infectado que incluya referencias a controles OLE/COM diseñados para explotar la vulnerabilidad.

A diferencia de otros fallos recientes, esta vulnerabilidad no afecta al "Panel de Vista Previa" (Preview Panel), lo que significa que el archivo debe ser abierto por el usuario para que el ataque tenga éxito.

Esta vulnerabilidad ya está siendo utilizada en campañas maliciosas, principalmente a través de correos electrónicos de phishing. Debido a la amplia adopción de Microsoft Office en entornos corporativos, el impacto potencial es elevado y afecta directamente a estaciones de trabajo de usuarios finales.

Productos afectados:

La vulnerabilidad tiene un alcance amplio, afectando tanto a versiones locales como basadas en la nube:

- Microsoft 365 Apps for Enterprise (32 y 64 bits).
- Microsoft Office LTSC 2024 y LTSC 2021.
- Microsoft Office 2019 (32 y 64 bits). Build 16.0.10417.20095
- Microsoft Office 2016 (32 y 64 bits). Build 16.0.5539.1001

Modo de explotación y cadena de infección

La vulnerabilidad permite a un atacante evadir las protecciones de seguridad que normalmente restringen la ejecución de controles COM y objetos OLE maliciosos.

Existe un error de lógica en la validación de las cabeceras de seguridad de archivos compuestos. El atacante manipula estas cabeceras para engañar a Office, haciendo que la aplicación considere un objeto peligroso como "confiable".

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

El atacante envía un documento de Office (.docx, .xlsx, etc.) especialmente diseñado mediante técnicas de *spear-phishing*. Al abrirlo, el archivo elude el modo de Vista Protegida y la "Marca de la Web" (MotW), permitiendo que el objeto malicioso se instancie y ejecute código en el contexto del usuario local.

El uso de esta vulnerabilidad suele alinearse con las siguientes tácticas y técnicas de ataque (MITRE ATT&CK Mapping):

- T1566.001 (Phishing: Attachment): Envío de documentos maliciosos por correo electrónico.
- T1204.002 (User Execution: Malicious File): Requiere que el usuario final abra el archivo para iniciar la cadena de infección.
- T1129 (Shared Modules): Carga de controles COM/OLE vulnerables para evadir restricciones del sistema.

Recomendaciones de mitigación:

- Dado que el vector de ataque inicial depende de la interacción del usuario a través de técnicas de *phishing* e ingeniería social, es imperativo reforzar las capacidades de detección de los colaboradores. Se recomienda al departamento de TI emitir una alerta de seguridad que instruya al personal a:

  – Verificar exhaustivamente la identidad del remitente antes de abrir archivos adjuntos.
  – Desconfiar de correos no solicitados o con un sentido de urgencia inusual, incluso si provienen de fuentes aparentemente legítimas.
  – Reportar de inmediato cualquier comunicación sospechosa al equipo de Respuesta a Incidentes (SOC/TI) sin interactuar con el contenido.

- Office 2021, LTSC 2021, LTSC 2024 y Microsoft 365 Apps

La corrección será automáticamente a través de un cambio del lado del servidor, pero tendrá que reiniciar Office para que el parche surta efecto.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Office 2016

  Proceder con la instalación de las actualizaciones correspondientes a través de MECM/SCCM, WSUS o la Herramienta de Implementación de Office (ODT), según la arquitectura tecnológica de la entidad. En caso de no ser posible el despliegue automatizado, se recomienda realizar la instalación manual descargando el paquete de actualización desde el siguiente enlace:
  https://support.microsoft.com/es-es/topic/descripci%C3%B3n-de-la-actualizaci%C3%B3n-de-seguridad-para-office-2016-26-de-enero-de-2026-kb5002713-32ec881d-a3b5-470c-b9a5-513cc46bc77e

- Office 2019

La solución permanente es actualizar a la Build 16.0.10417.20095 (o superior), para esto puede seguir los siguientes pasos:

- Abre cualquier aplicación de Office (Word, Excel, etc.).
- Ve a Archivo > Cuenta.
- En la sección Información del producto, busca Acerca de Word (o la aplicación que tengas abierta).
- Compara el número de versión. Si es inferior a 16.0.10417.20095, haz clic en Opciones de actualización > Actualizar ahora.

Para despliegue de la actualización por política se recomienda usar la opción de ODT o SCCM con la versión específica mencionada antes, ya que esto garantiza que el equipo llegue exactamente a la build que corrige la vulnerabilidad y no dependa de que el usuario haga clic en "Actualizar ahora".

En caso de no poder desplegar la actualización o realizar la instalación de la misma, Microsoft recomienda realizar la siguiente configuración en el regedit para mitigar la vulnerabilidad.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

1. Cierre todas las aplicaciones de Microsoft Office.
2. Cree una copia de seguridad del Registro de Windows, ya que editarlo incorrectamente puede causar problemas con el sistema operativo.
3. Abra el Editor del Registro de Windows (regedit.exe) haciendo clic en el menú Inicio y escribiendo regedit, luego presione Entrar cuando aparezca en los resultados de la búsqueda.
4. Una vez abierto, utilice la barra de direcciones en la parte superior para ver si existe una de las siguientes claves de registro:

   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\Common\COM Compatibility\ (for 64-bit Office, or 32-bit Office on 32-bit Windows)
   - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Common\COM Compatibility\ (for 32-bit Office on 64-bit Windows)
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Microsoft\Office\16.0\Common\COM Compatibility\
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\WOW6432Node\Microsoft\Office\16.0\Common\COM Compatibility\

   Si una de las claves anteriores no existe, cree una nueva clave de " Compatibilidad COM " en esta ruta de Registro haciendo clic derecho en Común y seleccionando Nuevo -> Clave.

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\Common\

5. Ahora haga clic derecho en la clave de compatibilidad COM existente o recién creada y seleccione Nuevo -> Clave y nómbrela {EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B} .

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

6. Cuando se cree el nuevo {EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B} , haga clic derecho sobre él y seleccione Nuevo -> Valor DWORD (32 bits) . Nombre el nuevo valor como Indicadores de compatibilidad.
7. Cuando se crea el valor de Indicadores de compatibilidad, haga doble clic en él, asegúrese de que la opción Base esté configurada en Hexadecimal e ingrese 400 en el campo de datos Valor.

Fuentes:

- https://thehackernews.com/2026/01/microsoft-issues-emergency-patch-for.html
- https://www.cve.org/CVERecord?id=CVE-2026-21509
- https://www.bleepingcomputer.com/news/microsoft/microsoft-patches-actively-exploited-office-zero-day-vulnerability/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21509

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570