Alerta

Técnica

Vulnerabilidad en Microsoft Office

COLCERT AL - 20260205 - 093

TLP:CLEAR

Resumen Ejecutivo

Se ha divulgado una vulnerabilidad de seguridad de severidad alta en **Microsoft Office**, identificada como **CVE-2026-21509**, que permite eludir mecanismos de protección y la ejecución remota de código arbitrario mediante el procesamiento de documentos especialmente diseñados en formatos RTF/DOC. La falla se origina por un manejo inseguro de contenido externo, permitiendo que un archivo malicioso fuerce la descarga y ejecución de cargas útiles desde servidores remotos sin requerir macros ni interacción adicional del usuario.

NIVEL DE RIESGO

ALTO

Dado que **Microsoft Office** constituye una de las plataformas de productividad más ampliamente utilizadas en entidades gubernamentales, sector financiero, salud, educación y empresas privadas en Colombia, la explotación de esta vulnerabilidad representa un vector de alto riesgo para la región, especialmente en escenarios de campañas de phishing dirigidas o ataques de ingeniería social. Un compromiso exitoso podría facilitar el robo de información sensible, la ejecución de malware, el movimiento lateral dentro de redes corporativas y la afectación de la continuidad operativa institucional.

Vulnerabilidad identificada

CVE	Producto afectado	Score CVSS	Descripción	CISA KEV
CVE-2026-21509	Microsoft 365 Apps: • 16.0.1. Office 2016: • 16.0.0 antes de 16.0.5539.1001 Office 2019: • 19.0.0. Office 2021: • 16.0.1. Office 2024: • 16.0.1.	**7.8 (Alta)**	Vulnerabilidad que permite la ejecución remota de código mediante el procesamiento de documentos RTF/DOC especialmente manipulados. La falla se origina por un manejo inseguro de contenido externo, permitiendo que el archivo fuerce conexiones para descargar y ejecutar cargas maliciosas sin requerir macros ni interacción adicional del usuario. Un atacante puede distribuir documentos a través de campañas de *phishing* para comprometer equipos, instalar *malware*, capturar información sensible y obtener persistencia dentro de la red. La vulnerabilidad ya se encuentra en explotación activa, incrementando el riesgo de campañas automatizadas y dirigidas contra organizaciones.	**TRUE**

Comunicado de Microsoft

Microsoft ha publicado un boletín de seguridad de emergencia fuera del ciclo regular para abordar la vulnerabilidad **CVE-2026-21509** en Microsoft Office, clasificada como un “Security Feature Bypass” con un puntaje CVSS de 7.8 (Alta). La compañía confirmó que esta falla fue identificada internamente por sus equipos de seguridad y que estaba siendo explotada activamente en la naturaleza en el momento de su divulgación, lo que motivó la liberación de actualizaciones para mitigar el riesgo inmediato.

Los parches están disponibles para versiones como **Office 2016**, **Office 2019** y **Microsoft 365 Apps for Enterprise**, mientras que en algunas versiones más recientes las protecciones se aplican automáticamente desde el lado del servicio, aunque se requiere reiniciar las aplicaciones para activarlas.

¿Cómo podría aprovechar esta vulnerabilidad un ciberdelincuente?

1. **Distribución del documento malicioso:** un actor de amenazas envía correos electrónicos de *phishing* con archivos RTF/DOC diseñados para explotar la vulnerabilidad en Microsoft Office, haciéndose pasar por comunicaciones legítimas (facturas, notificaciones administrativas, contratos o reportes internos).

2. **Ejecución automática del exploit al abrir el archivo:** al visualizar el documento, la aplicación procesa contenido externo de forma insegura y puede establecer conexiones WebDAV/HTTP hacia servidores controlados por el atacante, permitiendo la descarga de código malicioso sin necesidad de habilitar macros o realizar acciones adicionales.

3. **Acceso inicial sin credenciales:** el ciberdelincuente no requiere contraseñas ni autenticación previa. Basta con que la víctima abra el archivo para que se produzca la ejecución remota de código en el equipo comprometido, facilitando una intrusión rápida y silenciosa.

4. **Instalación de *malware* y persistencia:** tras la explotación, el atacante puede desplegar cargas adicionales, crear tareas programadas o modificar el registro del sistema para mantener acceso persistente y evadir controles de seguridad.

5. **Captura de información sensible:** el acceso al sistema permite capturar credenciales, correos electrónicos, documentos internos, tokens de sesión y otra información estratégica almacenada o accesible desde el equipo afectado.

6. **Movimiento lateral dentro de la red:** utilizando credenciales comprometidas o técnicas de escalamiento de privilegios, el actor de amenazas puede propagar su operación a otros dispositivos, servidores o servicios corporativos, ampliando el impacto del incidente.

7. **Uso del equipo como punto de apoyo para ataques posteriores:** el sistema comprometido puede emplearse como base para exfiltración de datos, espionaje prolongado, despliegue de *ransomware* o sabotaje operativo, comprometiendo la confidencialidad, integridad y disponibilidad de la organización.

Explotación actual por parte de APT28

El grupo de ciberespionaje **APT28** (también conocido como "Fancy Bear", vinculado a la inteligencia militar rusa) ha comenzado a atacar esta **falla de seguridad** a través de la campaña denominada **"Operación Neusploit"**

Aunque esta campaña está dirigida principalmente a objetivos en Europa central y oriental (incluidos Ucrania, Eslovaquia y Rumania), **la vulnerabilidad técnica es universal**. Esto indica que, cualquier organización a nivel global que utilice Microsoft Office sin actualizar estaría expuesta a esta amenaza por parte de criminales o el mismo APT, si este decide ampliar sus objetivos.

Tenga en cuenta que la vulnerabilidad (CVE-2026-21509) se hizo pública hace menos de dos semanas. Sorprendentemente, **APT28 comenzó a explotarla masivamente al tercer día** de su descubrimiento, lo que demuestra una capacidad de reacción extremadamente peligrosa.

Detalles de la explotación de APT28

- **Vector de Ataque:** Spear-phishing con archivos adjuntos maliciosos de tipo RTF (documento con formato de texto enriquecido). Por otro lado, los señuelos de ingeniería social se crearon tanto en inglés como en idiomas localizados (rumano, eslovaco y ucraniano) para apuntar a los usuarios de los respectivos países.
- **Vulnerabilidad: CVE-2026-21509** (CVSS 7.8). Se trata de un fallo de "omisión de característica de seguridad" que permite evadir las mitigaciones OLE (mecanismos de seguridad de Microsoft Office diseñados para proteger contra la ejecución de código malicioso).
- **Modus Operandi:** Al abrir el archivo, el exploit fuerza una petición para descargar cargas útiles adicionales. No requiere interacción compleja más allá de abrir el archivo (la Vista Previa no es un vector directo, pero el usuario debe ejecutar el documento).
- Después de ello hay dos caminos, se ejecuta **MiniDoor**, un ladrón de correo electrónico basado en macros de Outlook, o se ejecuta **PixyNetLoader**, el cual implanta **Covenant Grunt** (establece comando y control) a través de una imagen (esteganografía).

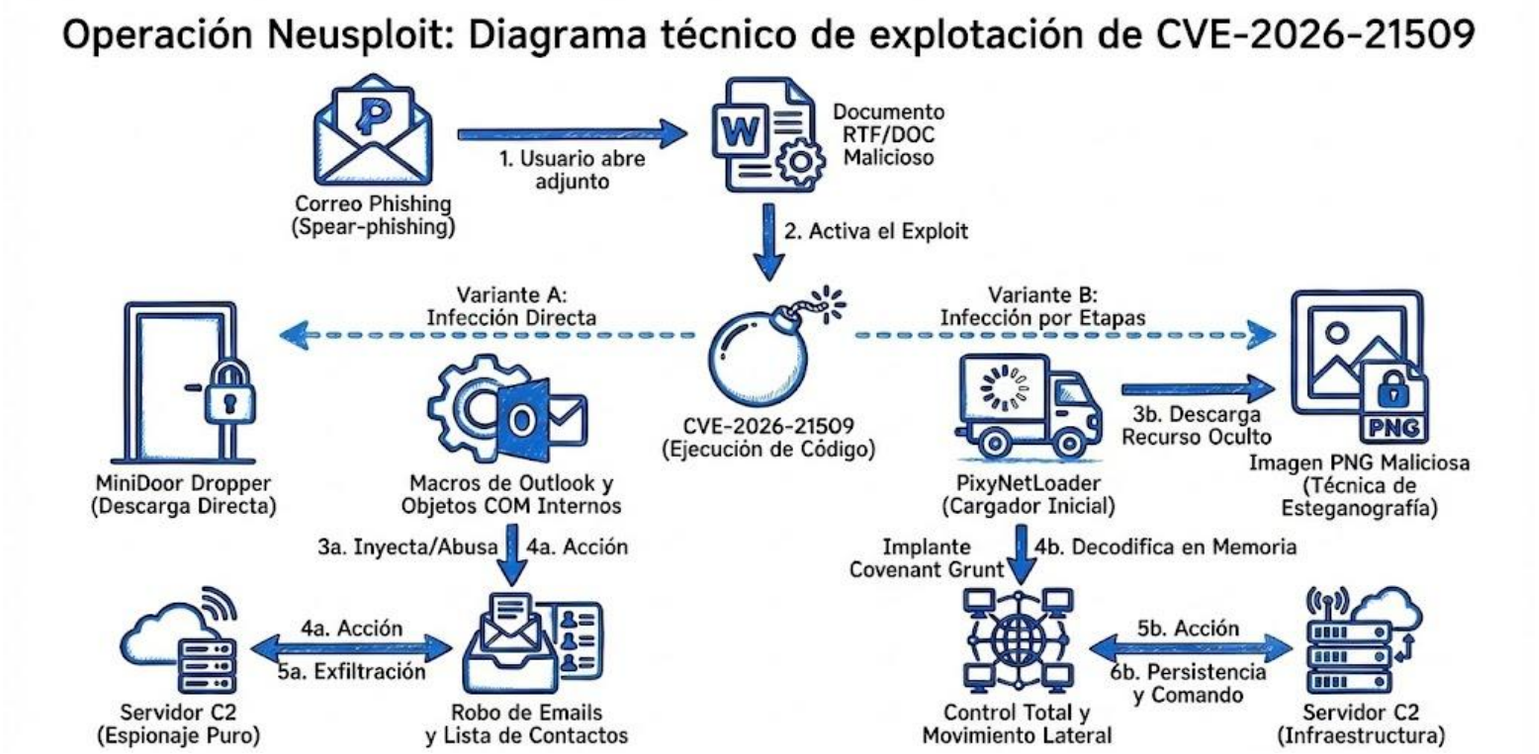

***Figura 1**: Diagrama de flujo que ilustra la secuencia de ataque, desde la ingeniería social hasta el comando y control del atacante.*

IoCs identificados para la explotación de APT28

Tipo de indicador	Valor / Indicador	Descripción
Hash	95e59536455a089ced64f5af2539a449 4592e6173a643699dc526778aa0a30330d16fe08 b2ba51b4491da8604ff9410d6e004971e3cd9a321390d0258e294ac42010b546	Archivo RTF que aprovecha CVE-2026-21509
Hash	2f7b4dca1c79e525aef8da537294a6c4 c4799d17a4343bd353e0edb0a4de248b99295d4d 1ed863a32372160b3a25549aad25d48d5352d9b4f58d4339408c4eea69807f50	Archivo RTF que aprovecha CVE-2026-21509
Hash	4727582023cd8071a6f388ea3ba2feaa d788d85335e20bb1f173d4d0494629d36083dddc 5a17cfaea0cc3a82242fdd11b53140c0b56256d769b07c33757d61e0a0a6ec02	Archivo RTF que aprovecha CVE-2026-21509
Hash	d47261e52335b516a777da368208ee91 c8c84bf33c05fb3a69bc5e2d6377b73649b93dce fd3f13db41cd5b442fa26ba8bc0e9703ed243b3516374e3ef89be71cbf07436b	Archivo RTF que aprovecha CVE-2026-21509
Hash	7c396677848776f9824ebe408bbba943 D577c4a264fee27084ddf717441eb89f714972a5 c91183175ce77360006f964841eb4048cf37cb82103f2573e262927be4c7607f	Archivo RTF que aprovecha CVE-2026-21509
Hash	f3b869a8d5ad243e35963ba6d7f89855 c1b272067491258ea4a2b1d2789d82d157aaf90a a944a09783023a2c6c62d3601cbd5392a03d808a6a51728e07a3270861c2a8ee	DLL dropper (variante 1) para MiniDoor
Hash	f05d0b13c633ad889334781cf4091d3e 7bbb530eb77c6416f02813cd2764e49bd084465c bb23545380fde9f48ad070f88fe0afd695da5fcae8c5274814858c5a681d8c4e	MiniDoor
Hash	859c4b85ed85e6cc4eadb1a037a61e16 da1c3e92f69e6ca0e4f4823525905cb6969a44ad 0bb0d54033767f081cae775e3cf9ede7ae6bea75f35fbfb748ccba9325e28e5e	DLL dropper PixyNetLoader (variante 2)
Hash	e4a5c4b205e1b80dc20d9a2fb4126d06 e52a9f004f4359ea0f8f9c6eb91731ed78e5c4d3 a876f648991711e44a8dcf888a271880c6c930e5138f284cd6ca6128eca56ba1	Cargador de código shell
Hash	154ff6774294e0e6a46581c8452a77de 22da6a104149cad87d5ec5da4c3153bebf68c411 2822c72a59b58c00fc088aa551cdeeb92ca10fd23e23745610ff207f53118db9	Archivo PNG que contiene código shell incrustado mediante esteganografía
Hash	ee0b44346db028a621d1dec99f429823 cea7e9323d79054f92634f4032c26d30c1cedd7e 9f4672c1374034ac4556264f0d4bf96ee242c0b5a9edaa4715b5e61fe8d55cc8	Archivo de configuración de tareas programadas de Windows
Hash	ea6615942f2c23dba7810a6f7d69e2da 23b6f9c00b9d5475212173ec3cbbcff34c4400a7 3f446d316efe2514efd70c975d0c87e12357db9fca54a25834d60b28192c6a69	Implanta Covenant Grunt que utiliza la API Filen como C2Bridge
Dominio	freefoodaid[.]com	Dominio malicioso
Dominio	wellnesscaremed[.]com	Dominio malicioso
URL	hxxps://freefoodaid[.]com/documents/2_2.d	URL que aloja MiniDoor dropper DLL
URL	hxxps://freefoodaid[.]com/tables/tables.d	URL que aloja PixyNetLoader
URL	hxxps://freefoodaid[.]com/documents/2_2.lNk	URL que aloja LNK

Impacto para Colombia y la región

- **Sectores afectados**: gobierno, financiero, educación, defensa, industria, transporte, comunicaciones, tecnologías de la información y comunicaciones.
- **Riesgo alto:** el nivel de riesgo asociado a esta vulnerabilidad se considera alto para Colombia y la región, ya que la explotación puede activarse simplemente con la apertura de un archivo ofimático malicioso, reduciendo la necesidad de técnicas complejas de intrusión.
- **Posibles consecuencias:**
  - Ejecución remota de *malware*, instalación de backdoors y establecimiento de persistencia en equipos institucionales.
  - Captura de credenciales corporativas, correos electrónicos, documentos internos y bases de datos confidenciales.
  - Exfiltración masiva de información o preparación del entorno para ataques posteriores, incluyendo *ransomware* o sabotaje operativo.

Implicaciones en seguridad nacional y de la región: dado que Microsoft Office es una herramienta transversal en la administración pública y en operadores de infraestructura crítica, la explotación exitosa de esta vulnerabilidad podría facilitar campañas de espionaje, filtración de información estratégica o compromisos simultáneos en múltiples entidades, debilitando la capacidad de respuesta ante incidentes y afectando la confianza en los servicios digitales del Estado y del sector productivo.

Técnicas MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Phishing: Spearphishing Attachment	**T1566.001**	El atacante envía documentos Office maliciosos (.RTF/.DOC) por correo electrónico que, al ser abiertos por la víctima, activan la explotación de la vulnerabilidad para lograr acceso inicial al sistema.
Ingress Tool Transfer	**T1105**	El sistema comprometido descarga herramientas o binarios maliciosos desde servidores externos controlados por el atacante para ampliar las capacidades del acceso inicial.
Exfiltration Over C2 Channel	**T1041**	La información sensible recopilada puede ser enviada a servidores de comando y control mediante canales cifrados o tráfico web aparentemente legítimo.

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Update Software	**M1051**	Aplicar de forma inmediata los parches y actualizaciones de seguridad de Microsoft Office que corrigen CVE-2026-21509, eliminando el vector principal de explotación.
User Training	**M1017**	Capacitar a los usuarios para identificar correos de *phishing* y archivos sospechosos, reduciendo la probabilidad de apertura de documentos maliciosos.
Privileged Account Management	**M1026**	Aplicar el principio de mínimo privilegio y restringir cuentas administrativas para reducir el impacto de la explotación y el escalamiento de privilegios.

Recomendaciones

- ❑ Instalar los parches oficiales liberados por Microsoft Office que corrigen **CVE-2026-21509** en todas las estaciones de trabajo y servidores donde se utilicen aplicaciones de Office, priorizando equipos expuestos a correo electrónico o acceso a Internet.
- ❑ Asegurar que Microsoft 365 Apps y versiones soportadas de Office reciban parches de seguridad de manera continua para reducir la ventana de exposición ante futuras vulnerabilidades.
- ❑ Configurar filtros de correo electrónico y pasarelas de seguridad para bloquear o poner en cuarentena documentos ofimáticos provenientes de fuentes no confiables o externas.
- ❑ Limitar conexiones desde estaciones de usuario hacia servidores externos no autorizados para prevenir la descarga automática de cargas maliciosas durante la explotación.
- ❑ Reforzar campañas de concienciación para que el personal identifique correos sospechosos, adjuntos inesperados o solicitudes inusuales relacionadas con documentos.
- ❑ En caso de sospecha de compromiso, cambiar contraseñas, claves API y sesiones activas para evitar persistencia del atacante.

Fuentes

Microsoft MSRC (Microsoft Security Response Center), 28 de enero de 2026, CVE-2026-21509 – Microsoft Office Security Feature Bypass Vulnerability, boletín oficial del fabricante con detalles técnicos, productos afectados y actualizaciones de seguridad.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509.

CVE Program (CVE.org), 26 de enero de 2026, CVE-2026-21509, registro oficial de la vulnerabilidad con clasificación, métricas CVSS y descripción técnica estandarizada.
https://www.cve.org/CVERecord?id=CVE-2026-21509

Cybersecurity and Infrastructure Security Agency (CISA), 2026, Known Exploited Vulnerabilities Catalog, catálogo gubernamental que lista vulnerabilidades con evidencia de explotación activa.
https://www.cisa.gov/known-exploited-vulnerabilities-Catalog.

The Hacker News, 3 de febrero de 2026, APT28 Uses Microsoft Office CVE-2026-21509 in Espionage-Focused Malware Attacks, reporte periodístico y análisis de la explotación activa de la vulnerabilidad en campañas reales.
https://thehackernews.com/2026/02/apt28-uses-microsoft-office-cve-2026.html.

CISA (Cybersecurity & Infrastructure Security Agency), 4 de febrero de 2026, *Known Exploited Vulnerabilities Catalog*, base de datos oficial de vulnerabilidades con explotación activa confirmada y directrices de mitigación para agencias federales.
https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

Zscaler, 3 de febrero de 2026, *APT28 Leverages CVE-2026-21509 in Operation Neusploit*, investigación técnica detallada sobre la infraestructura de comando y control y el despliegue de malware en la campaña Neusploit.
https://www.zscaler.com/blogs/security-research/apt28-leverages-cve-2026-21509-operation-neusploit.