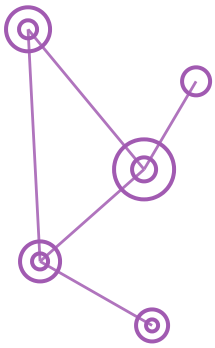
bitnaga
AI-native cybersecurity

TLP:CLEAR



INFORME DE SEGUIMIENTO · ZERO-DAY EXPLOTADO

CVE-2026-124194

Vulnerabilidad en Microsoft Outlook explotada activamente que permite robar credenciales de los empleados. Situación, exposición y decisiones para dirección.

CÓDIGO	FECHA	VERSIÓN	ÁREA
SEG-2026-1124	14.11.2026	1.0	Dirección / CISO

1. Resumen para dirección

Una vulnerabilidad «moderada» que ya se está usando en ataques reales.

El 10 de noviembre Microsoft corrigió un fallo en Outlook (CVE-2026-124194) que permite a un atacante obtener las credenciales de un empleado con solo conseguir que abra un fichero preparado. Microsoft confirma que la vulnerabilidad ya se explotaba antes del parche y la agencia estadounidense de ciberseguridad (CISA) la incluyó ese mismo día en su catálogo de vulnerabilidades explotadas.

Su puntuación oficial es baja (CVSS 6,5), pero el riesgo real no lo es: está activa, afecta a la herramienta de trabajo diaria de casi toda la plantilla y lo que roba —credenciales— es la puerta de entrada habitual a incidentes mayores.

Decisión que se solicita. Tratar esta actualización como urgente: desplegar el parche de Office en toda la organización en un plazo máximo de **72 horas** y confirmar la cobertura antes del **24 de noviembre**, fecha límite fijada por CISA.

2. Estado actual

INDICADOR	SITUACIÓN	FECHA
Explotación activa	**Sí**, confirmada por Microsoft	10.11.2026
Catálogo KEV de CISA	Incluida · plazo de corrección 24.11	10.11.2026
Parche	Disponible (actualización de Office)	10.11.2026
Severidad oficial	Moderada · CVSS 6,5	—
Código de ataque público (PoC)	No detectado a fecha de este informe	14.11.2026
Autoría y alcance de la campaña	No divulgados por Microsoft	—

3. Qué ocurre, sin tecnicismos

01 El atacante envía o hace llegar a un empleado un fichero de Office manipulado.

02 Al abrirlo, Outlook contacta en segundo plano con un servidor del atacante **sin mostrar el aviso de seguridad** que normalmente lo impediría.

03 En esa conexión, el equipo entrega una «huella» cifrada de la contraseña del empleado (técnicamente, un *hash* NTLMv2).

04 Con esa huella, el atacante puede **hacerse pasar por el empleado** ante otros sistemas internos o intentar descifrarla para obtener la contraseña real.

Es el equivalente a que un visitante consiga una copia de la tarjeta de acceso de un empleado sin que este lo note. No hace falta que el atacante esté dentro de la red: basta con que el empleado abra el fichero.

4. Por qué la puntuación engaña

La puntuación CVSS mide la gravedad técnica teórica de un fallo, no si alguien lo está aprovechando. En este caso, dos señales pesan más que el 6,5:

- **Ya hay ataques en curso.** Microsoft lo ha detectado y CISA lo ha catalogado el mismo día de la publicación.
- **El botín son credenciales.** Una identidad robada permite moverse por la organización con apariencia legítima, lo que retrasa la detección y amplifica el daño.

Por eso recomendamos priorizar por estado de explotación y no por puntuación.

5. Exposición de la organización

Están afectados los equipos con **Microsoft 365 Apps for Enterprise** y **Office LTSC 2021 y 2024**, es decir, prácticamente todos los puestos de trabajo con Outlook de escritorio. Preguntas que conviene trasladar al equipo técnico:

PREGUNTA PARA EL EQUIPO TÉCNICO	POR QUÉ IMPORTA
¿Qué porcentaje de equipos tiene ya la actualización de noviembre?	Es la única corrección completa.
¿Se bloquean las conexiones salientes de compartición de ficheros (SMB, puerto 445) hacia internet?	Corta el canal por el que sale la huella de la contraseña.
¿Está restringido el uso de NTLM y protegidas las cuentas privilegiadas?	Limita lo que el atacante puede hacer con lo robado.
¿Vigila el SOC conexiones salientes anómalas desde Outlook?	Permite detectar si ya ha habido intentos.

6. Acciones recomendadas

ACCIÓN	RESPONSABLE	PLAZO
Desplegar la actualización de Office de noviembre	Sistemas	72 horas
Verificar y reportar la cobertura del parche	Sistemas	Antes del 24.11
Bloquear SMB saliente (TCP 445) en el perímetro	Redes	Inmediato
Aviso a la plantilla sobre ficheros adjuntos inesperados	Seguridad / Comunicación	Inmediato
Revisar actividad sospechosa desde Outlook y NTLM hacia el exterior	SOC	7 días
Restringir NTLM y proteger cuentas privilegiadas	Identidad	30 días

Mientras el parche no esté desplegado al 100 %, la concienciación y el filtrado del correo reducen el riesgo, porque el ataque requiere que el usuario abra el fichero.

7. Contexto: el ciclo de parches de noviembre

Este zero-day llega en uno de los mayores ciclos de actualización de Microsoft: más de mil vulnerabilidades corregidas, 63 de ellas críticas. Aunque no consten como explotadas, dos merecen atención paralela en los servidores:

- **Windows LDAP (CVE-2026-119958, CVSS 9,8):** pone en riesgo los controladores de dominio y el Directorio Activo.
- **Exchange Server (CVE-2026-118207, CVSS 9,8):** explotable por cualquiera capaz de enviar un correo a la organización.

Un dato relevante: Microsoft atribuye el descubrimiento de este fallo de Outlook a un investigador que utilizó un asistente de IA. Es una muestra de que la IA ya acelera tanto el hallazgo de vulnerabilidades como, previsiblemente, su explotación; los ciclos de parcheo deben acortarse en consecuencia.

8. Seguimiento

FECHA	HITO
10.11.2026	Publicación del parche e inclusión en el catálogo KEV
14.11.2026	Emisión de este informe (v1.0)
24.11.2026	Plazo de corrección fijado por CISA
08.12.2026	Próximo ciclo de parches de Microsoft

Actualizaremos este informe si se publica código de ataque, si se atribuye la campaña a un actor concreto o si se detecta actividad dirigida a organizaciones en España.

9. Fuentes

- Microsoft Security Response Center — Aviso CVE-2026-124194.
- CISA — Catálogo de vulnerabilidades explotadas conocidas (KEV), 10.11.2026.
- CSO Online — Análisis del Patch Tuesday de noviembre de 2026.
- Krebs on Security · CrowdStrike · Qualys — Análisis del ciclo de noviembre.