

Boletín de alerta

Boletín Nro.: 114

Fecha de publicación: 19/10/2026

Tema: Alerta 2026-114 Vulnerabilidades críticas en servicios de identidad, correo y red de Microsoft

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Componente	CVE	CVSS	Riesgo principal
Microsoft Outlook	CVE-2026-70242, CVE-2026-70291, CVE-2026-88156, CVE-2026-97016 y CVE-2026-97749	9.8	Ejecución remota de código sin autenticación. Para CVE-2026-70291 y CVE-2026-88156, el panel de lectura constituye un vector de ataque.
Microsoft QUIC	CVE-2026-100219 y CVE-2026-105016	9.8	Ejecución remota de código mediante tráfico dirigido a servicios que utilicen la implementación afectada de QUIC.
Windows DHCP Server	CVE-2026-96934	9.8	Ejecución remota de código mediante paquetes manipulados, sin credenciales ni interacción del usuario.
Windows Message Queuing Queue Manager	CVE-2026-100202	9.8	Ejecución remota de código mediante mensajes manipulados enviados al servicio MSMQ.
Microsoft PostScript Printer Driver	CVE-2026-70147 y CVE-2026-70153	9.8	Ejecución remota de código en servicios de impresión afectados, sin autenticación.
Microsoft Office PowerPoint	CVE-2026-88178	9.8	Ejecución de código al procesar una presentación manipulada; incluye escenarios de vista previa y Office Online afectado.
Active Directory Domain Services	CVE-2026-70229	8.1	Ejecución remota de código sin autenticación en controladores de dominio; complejidad de ataque alta.

Microsoft Exchange Server	CVE-2026-70571	8.1	Ejecución remota de código al procesar correo manipulado, sin interacción del usuario; complejidad alta.
Remote Desktop Gateway	CVE-2026-70187	8.1	Ejecución remota de código sin autenticación en el servicio de gateway; complejidad alta.
Windows Hyper-V	CVE-2026-102214 y CVE-2026-105733	8.8	Cruce de la frontera de virtualización desde una máquina invitada; requiere ejecución autenticada dentro de la VM.

Descripción

Se publicaron vulnerabilidades de severidad **crítica** que permiten ejecución remota de Código (RCE), suplantación de identidad y escalamiento de privilegios en productos empresariales en productos de Microsoft. Destacan las fallas en Outlook (CVE-2026-70242, CVE-2026-70291, CVE-2026-88156, CVE-2026-97016 y CVE-2026-97749), Microsoft QUIC (CVE-2026-100219 y CVE-2026-105016), DHCP Server (CVE-2026-96934), MSMQ (CVE-2026-100202) y PowerPoint (CVE-2026-88178), todas con CVSS 9.8. También se corrigieron vulnerabilidades en Active Directory Domain Services, Exchange Server y Remote Desktop Gateway, con CVSS 8.1, y en Hyper-V, con CVSS 8.8. Varias permiten ataques sin autenticación ni interacción del usuario, por lo que se recomienda priorizar la remediación de servicios expuestos, infraestructura de identidad y aplicaciones que procesan correo o documentos externos

A continuación se describen las vulnerabilidades principales:

1. Outlook y Office: compromiso mediante correo o contenido manipulado

Las cinco vulnerabilidades críticas de Outlook tienen una puntuación CVSS de 9.8. En particular, CVE-2026-70291 y CVE-2026-88156 pueden activarse al visualizar un mensaje manipulado en el panel de lectura, sin necesidad de abrir un adjunto o pulsar un enlace. Esto reduce la eficacia de medidas basadas únicamente en capacitación del usuario.

Office también presenta fallas críticas en PowerPoint, Word, Excel y Visio. Entre ellas, CVE-2026-88178 destaca por su puntuación de 9.8. No todas comparten el mismo vector: las vulnerabilidades críticas de Excel y Visio detalladas por CrowdStrike no consideran el panel de vista previa como vector de ataque.

La consecuencia principal es obtener ejecución de código en el contexto de la aplicación o usuario afectado, desde donde un atacante podría intentar acceder a información o continuar la intrusión.

• Active Directory: riesgo sobre la infraestructura de identidad

CVE-2026-70229 permite ejecución remota de código en Active Directory Domain Services mediante tráfico de red manipulado, sin autenticación ni interacción. Su explotación presenta complejidad alta y depende de condiciones de configuración y temporización; no debe describirse como un compromiso trivial de cualquier controlador de dominio.

También se corrigieron dos fallas críticas de suplantación en AD FS:

- CVE-2026-108131 — CVSS 7.5.
- CVE-2026-96222 — CVSS 7.4; relacionada con validación incorrecta de certificados.

Estos componentes requieren atención prioritaria por su función en la autenticación y en las relaciones de confianza de la organización.

• **QUIC, DHCP y MSMQ: ejecución de código sin credenciales**

Las vulnerabilidades de QUIC, DHCP Server y MSMQ permiten ataques de red sin autenticación sobre servicios afectados. La exposición depende de que el componente esté instalado, activo y sea alcanzable por el atacante.

En particular:

- QUIC: verificar servicios que utilicen la biblioteca afectada; no basta con identificar únicamente servidores web.
- DHCP Server: considerar la accesibilidad desde segmentos internos y mediante relays.
- MSMQ: identificar dependencias de aplicaciones empresariales y exposición de TCP/1801, su puerto habitual.

Que estos servicios no estén publicados en Internet no elimina el riesgo: pueden constituir objetivos de movimiento lateral desde un segmento interno comprometido.

• **Exchange y RD Gateway: servicios expuestos de alto valor**

CVE-2026-70571 afecta el procesamiento de contenido en Exchange Server y puede activarse mediante un correo especialmente manipulado. CVE-2026-70187 afecta Remote Desktop Gateway y permite ejecución remota de código mediante tráfico de red. Ambas requieren condiciones de explotación de complejidad alta, pero no autenticación.

La evaluación debe distinguir RD Gateway de otros despliegues de Escritorio remoto: no corresponde asumir que todo equipo con RDP habilitado presenta este mismo escenario.

• **Hyper-V: ruptura del aislamiento entre máquinas virtuales**

CVE-2026-102214 permite que un atacante con ejecución dentro de una VM afectada alcance el host Hyper-V. CVE-2026-105733 se relaciona con virtualización anidada y puede permitir alcanzar la máquina intermedia que actúa como hipervisor. No son ataques remotos directos contra cualquier host: requieren acceso previo dentro del entorno invitado.

Estado de explotación: distinción importante

La vulnerabilidad con explotación activa confirmada destacada en el reporte es CVE-2026-96951, un bypass de seguridad en Windows Shell que evade Mark of the Web. Microsoft la clasifica como importante, no crítica. Debe atenderse con urgencia por la evidencia de ataques, aunque no pertenezca al grupo principal de este boletín.

La confirmación de explotación de esa CVE no debe extenderse a las vulnerabilidades críticas enumeradas anteriormente. Severidad técnica, divulgación pública y explotación confirmada son criterios diferentes de priorización.

Solución

Se recomienda aplicar las actualizaciones de seguridad publicadas por Microsoft para cada producto y versión afectados, consultando las CVE correspondientes en Microsoft Security Update Guide para identificar los paquetes y requisitos aplicables.

Se sugiere priorizar los servicios expuestos a Internet, la infraestructura de identidad y los equipos que procesan correo o documentos externos; completar los reinicios requeridos y verificar posteriormente las versiones instaladas y la remediación mediante un análisis de vulnerabilidades. Mientras se implementan las correcciones, restringir el acceso a los servicios afectados y deshabilitar los componentes innecesarios puede reducir la exposición, pero no sustituye la instalación de los parches.

Para identificar productos afectados, requisitos, paquetes y versiones corregidas, consultar Microsoft Security Update Guide y buscar cada CVE:

<https://msrc.microsoft.com/security-guidance>

El portal de MSRC es la referencia oficial para determinar qué corrección corresponde a cada activo

Información adicional:

- <https://msrc.microsoft.com/security-guidance>
- <https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2026-patch-tuesday-fixes-1-411-flaws-3-zero-days/>
- <https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-october-2026/>
- <https://threatprotect.qualys.com/2026/10/14/microsoft-patch-tuesday-october-2026-security-update-review/>