

Boletín de alerta

Boletín Nro.: 99

Fecha de publicación: 11/09/2026

Tema: Alerta 2026-99 RCE crítica en Windows DNS Server — CVE-2026-69730

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

La vulnerabilidad afecta implementaciones de **Windows DNS Server** en sistemas Windows Server compatibles, incluyendo Windows Server 2012 y versiones posteriores, además de ciertas versiones de Windows 10 donde se ejecute el rol DNS. Las estaciones Windows 11 no figuran en el alcance difundido por los análisis de Patch Tuesday.

Componente	Producto afectado	Riesgo
Windows DNS Server	Windows Server 2012 y posteriores con el rol DNS habilitado	RCE remoto no autenticado
Windows DNS Server	Versiones Windows 10 1607 y 1809 con el rol DNS habilitado	RCE remoto no autenticado

El alcance definitivo por versión, arquitectura y KB aplicable debe validarse mediante la guía oficial de Microsoft para **CVE-2026-69730** y el catálogo de actualizaciones correspondiente al sistema operativo instalado.

Descripción

Se publicado, una vulnerabilidad crítica de **ejecución remota de código (RCE)** en Windows DNS Server, con puntuación **CVSS 9.8 etiquetada como CVE-2026-69730**. Un atacante remoto no autenticado puede enviar un paquete DNS especialmente diseñado al servicio afectado y ejecutar código en el sistema sin interacción del usuario; Microsoft estima que la explotación es **más probable**.

CVE-2026-69730 es una vulnerabilidad de tipo **use-after-free** en Windows DNS Server. El problema ocurre durante el procesamiento de paquetes DNS diseñados específicamente para activar el manejo incorrecto de memoria; como resultado, un atacante con conectividad de red al servicio DNS puede alcanzar ejecución remota de código.

La vulnerabilidad es especialmente sensible en entornos Active Directory, ya que es habitual que los **controladores de dominio también hospeden el rol DNS**. En esos casos, la explotación podría proporcionar

ejecución de código sobre un activo de identidad crítico, elevando significativamente el riesgo de compromiso de dominio, robo de credenciales, modificación de políticas, persistencia y movimiento lateral.

Solución

Aplicar inmediatamente las actualizaciones de seguridad de Microsoft de septiembre de 2026 en todos los servidores que ejecuten el rol Windows DNS Server. Priorizar controladores de dominio y servidores DNS expuestos o alcanzables desde redes de usuarios, VPN, WiFi, sucursales, DMZ y segmentos no confiables.

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-69730>

Recomendación Adicional:

No exponer Windows DNS Server directamente a Internet salvo que exista una necesidad operativa formal y controles compensatorios. Para zonas públicas, evaluar separar la función autoritativa pública de la infraestructura DNS interna y de Active Directory.

Información adicional:

- [Microsoft Security Response Center — CVE-2026-69730](#)
- [CrowdStrike — September 2026 Patch Tuesday: Updates and Analysis](#)
- [Tenable — Microsoft's September 2026 Patch Tuesday](#)
- [Zero Day Initiative — The September 2026 Security Update Review](#)
- [Cisco Talos — Microsoft Patch Tuesday for September 2026](#)