

Alert Bulletin

Bulletin N.: 99

Publication Date: 11/09/2026

Subject: Alert 2026-99 Critical RCE in Windows DNS Server — ~~CVE-2026-69730~~

Traffic Light Protocol (TLP): White

Affected product(s):

The vulnerability affects implementations of **Windows DNS Server** on supported Windows Server systems, including Windows Server 2012 and later versions, as well as certain versions of Windows 10 where the DNS role is running. Windows 11 workstations are not listed in the scope disclosed by the Patch Tuesday analyses.

Component	Affected Product	Risk
Windows DNS Server	Windows Server 2012 and later with the DNS role enabled	Unauthenticated remote RCE
Windows DNS Server	Windows 10 versions 1607 and 1809 with the DNS role enabled	Unauthenticated remote RCE

The definitive scope by version, architecture, and applicable KB must be validated through Microsoft's official guidance for ~~CVE-2026-69730~~ and the update catalog corresponding to the installed operating system.

Description

A critical **remote code execution (RCE)** vulnerability has been disclosed in Windows DNS Server, with a **CVSS score of 9.8 labeled as ~~CVE-2026-69730~~**. An unauthenticated remote attacker can send a specially crafted DNS packet to the affected service and execute code on the system without user interaction; Microsoft estimates that exploitation is **more likely**.

~~CVE-2026-69730~~ is a **use-after-free** vulnerability in Windows DNS Server. The issue occurs during the processing of DNS packets specifically designed to trigger incorrect memory handling; as a result, an attacker with network connectivity to the DNS service can achieve remote code execution.

The vulnerability is particularly sensitive in Active Directory environments, since it is common for **domain controllers to also host the DNS role**. In such cases, exploitation could provide code execution on a critical identity asset, significantly elevating the risk of domain compromise, credential theft, policy modification, persistence, and lateral movement.

Solution

Immediately apply the September 2026 Microsoft security updates on all servers running the Windows DNS Server role. Prioritize domain controllers and DNS servers exposed to or reachable from user networks, VPN, Wi-Fi, branch offices, DMZ, and untrusted segments.

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

Additional Recommendation:

Do not expose Windows DNS Server directly to the Internet unless there is a formal operational need and compensating controls. For public zones, consider separating the public authoritative function from the internal and Active Directory DNS infrastructure.

Additional information:

- [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](#)