Microsoft Fixes 80 Bugs, Including Two Maximum-Severity Vulnerabilities

TL;DR

Microsoft issued patches for 80 vulnerabilities in September 2025, including two CVSS 10 flaws affecting Azure Networking and Windows SMB.

Other high-severity bugs include remote code execution in HPC Pack and privilege escalation in NTLM. No active exploitation is reported, but the SMB flaw was publicly disclosed prior to patching.

Organizations should patch immediately and review SMB/NTLM configurations.

Overview

This week, Microsoft issued security updates addressing 80 vulnerabilities across Windows and other software. Eight are classified as “critical”, with the remainder rated “important”. Nearly half are privilege escalation flaws, demonstrating attackers’ continued focus on gaining higher-level access after initial compromise.

The most urgent vulnerabilities are CVE-2025-54914 and CVE-2025-55234, both scoring the maximum 10.0 on the CVSS scale. While Microsoft reports no active exploitation, the attack paths they expose could help launch destructive campaigns if left unpatched.

Vulnerability Breakdown

- **CVE-2025-54914** – Azure Networking Privilege Escalation (CVSS 10.0)
  A flaw in Azure Networking that could allow privilege escalation within cloud environments. Microsoft has already applied fixes to its infrastructure, meaning no customer action is required for remediation.

- **CVE-2025-55234** – Windows SMB Privilege Escalation (CVSS 10.0, Publicly Known)
  A flaw in Windows SMB authentication that allows attackers to conduct relay attacks if SMB signing and Extended Protection for Authentication (EPA) are not enforced. Successful exploitation could lead to elevation of privilege, credential theft, lateral movement, and data exfiltration. This vulnerability was already public prior to Microsoft’s patch release.

Other significant vulnerabilities this month include a remote code execution flaw in Microsoft HPC Pack (CVE-2025-55232, CVSS 9.8) and a privilege escalation vulnerability in Windows NTLM (CVE-2025-54918, CVSS 8.8). Additionally, BitLocker

and SQL Server received fixes for privilege escalation and denial-of-service flaws, respectively.

The SMB flaw is the vulnerability to focus on. It was already public, so attackers know about it. Aspire recommends that you patch now and lock down SMB settings.

Aspire Protects

- **Patch** - Apply all September 2025 patches immediately across Windows and Microsoft software. Put focus on CVE-2025-55234.
    - Audit SMB settings to enforce SMB signing and Extended Protection for Authentication (EPA).
    - Review NTLM configurations and monitor for unusual authentication attempts.
    - Harden BitLocker deployments by enabling TPM+PIN pre-boot authentication and applying REVISE mitigation to block downgrade paths.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – Attackers may attempt to exploit unpatched Windows services such as SMB or NTLM over exposed networks.

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548] – Vulnerabilities in NTLM and SMB could allow attackers to gain SYSTEM-level or administrative privileges.

Credential Access

- Credential Dumping [T1003] – Compromised NTLM or SMB relay attacks may provide adversaries access to stored credentials.

Lateral Movement

- SMB/Windows Admin Shares [T1021.002] – Attackers can use SMB relay to pivot across systems within the network.

Targeted Industries

The vulnerabilities patched this month affect core Windows and Azure services, making them relevant across all organizations that rely on Microsoft products for authentication, networking, or storage.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current

security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

September 2025 Security Updates - Release Notes - Security Update Guide - Microsoft

Support for Audit Events to deploy SMB Server Hardening—SMB Server Signing & SMB Server EPA - Microsoft Support

CVE-2025-55234 - Security Update Guide - Microsoft - Windows SMB Elevation of Privilege Vulnerability