Microsoft Patches Two Zero-Day Vulnerabilities

TL;DR

Microsoft patched two zero-day vulnerabilities: CVE-2025-33053 (CVSS 8.8), a WebDAV remote code execution flaw exploited in the wild by Stealth Falcon, and CVE-2025-33073 (CVSS 7.6), a Windows SMB client privilege escalation bug that was publicly disclosed.

Both issues can lead to full system compromise if left unpatched. Microsoft also addressed 64 additional vulnerabilities in this release, including ten critical remote code execution flaws.

Overview

Microsoft has patched two zero-day vulnerabilities (CVE-2025-33053 and CVE-2025-33073) that could allow attackers to gain unauthorized access or control over Windows systems.

Vulnerability Breakdown

- CVE-2025-33053 – WebDAV Remote Code Execution (CVSS 8.8)
  This vulnerability allows attackers to execute code remotely when a user clicks a malicious WebDAV link. It was exploited in the wild by Stealth Falcon, an APT group that targeted a defense contractor in Turkey. The attackers abused a built-in Windows utility to execute files from a remote WebDAV server without authentication. Microsoft confirmed the bug and issued a fix.

- CVE-2025-33073 – Windows SMB Client Privilege Escalation (CVSS 7.6)
  This vulnerability was publicly disclosed prior to patch availability. It allows attackers to trick a vulnerable machine into connecting to a rogue SMB server. Once the connection is made, the attacker can elevate privileges to SYSTEM. Though exploitation has not been confirmed in the wild, DFN-CERT and RedTeam Pentesting have issued public warnings.

Affected Products

- Windows 10 and 11 (all supported builds)
- Windows Server 2016, 2019, and 2022
- Microsoft SMB Client
- Microsoft WebDAV Service
- Microsoft Office, SharePoint, Excel, Outlook, Word

In total, Microsoft addressed 66 vulnerabilities in this update cycle, including 10 rated critical. The remaining issues affect components like Office, SharePoint, DHCP, and Windows Installer. Zero-day bugs keep hitting file sharing and collaboration tools like WebDAV and SMB. If these are part of your environment, Aspire recommends that you patch immediately.

Aspire Protects

- **Patch –** Apply the June 2025 Microsoft patches immediately on all endpoints and servers.
    - CVE-2025-33073 - See Microsoft's Advisory for patch guidance.
        - Enforce SMB signing through Group Policy to mitigate CVE-2025-33073 if patching is delayed.
        - Use firewall rules to block outbound SMB (TCP 445) where not required.
        - Monitor for anomalous outbound SMB traffic that may indicate privilege escalation attempts via rogue SMB servers.
    - CVE-2025-33053 - See Microsoft's Advisory for patch guidance.
        - Disable WebDAV services on endpoints and servers if not actively in use.
        - Block outbound WebDAV traffic at the network perimeter to prevent callback attempts.
        - Monitor logs for unusual WebDAV activity, especially user-initiated file execution from remote URLs.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may have used a malicious WebDAV link to launch remote code execution against targeted systems.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may have coerced SMB authentication to gain elevated privileges on a victim machine.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how

we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

These vulnerabilities are especially concerning for organizations that rely on Windows file-sharing protocols and WebDAV for collaboration or application delivery.

- Defense and Aerospace
- Government
- Financial Services
- Education
- Healthcare
- Legal & Professional Services

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

NVD - CVE-2025-33053

CVE-2025-33073 - Security Update Guide - Microsoft - Windows SMB Client Elevation of Privilege Vulnerability

CVE-2025-33053 - Security Update Guide - Microsoft - Web Distributed Authoring and Versioning (WEBDAV) Remote Code Execution Vulnerability

NVD - CVE-2025-33053

CVE-2025-33053: RCE in WebDAV | Kaspersky official blog

CVE-2025-33073: Windows SMB Client Zero-Day Lets Attackers Gain SYSTEM Privileges | SOC Prime