Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Microsoft September 2025 Patch Tuesday Addresses Critical NTLM and Office Vulnerabilities

Vulnerability Note: VN-2025-26

Date of Issue: 12 September 2025

Severity Rating: High

Systems Affected:

- Microsoft Windows operating systems (multiple versions)
- Microsoft Office Suite (multiple versions)
- Windows Server components
- Microsoft Hyper-V

Description

Microsoft has released its September 2025 Patch Tuesday updates, addressing 81 security vulnerabilities across its product portfolio. Among these, 13 vulnerabilities are rated as Critical, with the most severe being a Windows NTLM authentication flaw that could allow attackers to elevate privileges over a network.

The most critical vulnerability (CVE-2025-54918) affects Windows NTLM (NT LAN Manager), a suite of code for managing authentication in Windows network environments. This improper authentication vulnerability allows an authorized attacker to elevate privileges over a network. Microsoft has rated this flaw as "Exploitation More Likely," and security researchers note that it could be exploited over the network or Internet, potentially allowing attackers to gain SYSTEM-level privileges on target machines.

Another critical vulnerability (CVE-2025-54910) affects Microsoft Office and could allow remote code execution when a user opens a specially crafted Office document. This vulnerability has a CVSS score of 8.4 and requires no user interaction beyond opening a malicious file.

Additionally, Microsoft addressed a publicly disclosed zero-day vulnerability (CVE-2025-55234) affecting the Windows SMB protocol, which could allow attackers to perform relay attacks leading to privilege escalation. While not currently under active exploitation, its public disclosure status increases the risk for opportunistic attacks.

CVE Information

CVE-2025-54918

CVE-2025-54910
CVE-2025-55234
CVE-2025-54916

Mitigation

Microsoft recommends that organizations apply the September 2025 security updates immediately. Key mitigation steps include:

1. Priority Patching: Focus on the critical vulnerabilities first, particularly CVE-2025-54918 (Windows NTLM) and CVE-2025-54910 (Microsoft Office RCE)

2. SMB Hardening: For CVE-2025-55234, enable SMB Server Signing and Extended Protection for Authentication (EPA) where possible. Microsoft has introduced new audit capabilities to help assess compatibility before enforcing SMB hardening

3. Office Security: Implement email filtering and document inspection to prevent malicious Office documents from reaching users. Educate users about the risks of opening unexpected attachments

4. NTFS Protection: For CVE-2025-54916, ensure proper file system permissions and user education about social engineering attacks involving malicious files

5. Update Management: Ensure automatic updates are enabled for all Microsoft products and verify that systems have successfully installed the September 2025 patches

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene