Posted Date: 2025/10/29

[Vulnerability Alert] Windows SMB has a high-risk security vulnerability (CVE-2025-33073), please confirm and patch as soon as possible

- Subject: [Vulnerability Alert] Windows SMB has a high-risk security vulnerability (CVE-2025-33073), please confirm and patch as soon as possible
- Content:
  - Forwarded from National Information Security Information Sharing and Analysis Center NISAC-200-202510-00000308
  - Researchers have discovered an NTLM Reflection vulnerability (CVE-2025-33073) in the Windows SMB client. A remote attacker with general user privileges can execute a malicious script to force the SMB client to connect and authenticate with an attacker-controlled SMB server. Due to a flaw in the SMB client's authentication phase, the attacker can bypass security checks to elevate privileges to System level, thereby gaining control of the client system. This vulnerability has already been exploited by hackers, so please confirm and patch it as soon as possible.
- Affected Platforms:
  - Windows Server 2025 (Server Core installation)
  - Windows Server 2025
  - Windows Server 2022, 23H2 Edition (Server Core installation)
  - Windows Server 2022 (Server Core installation)
  - Windows Server 2022
  - Windows Server 2019 (Server Core installation)
  - Windows Server 2019
  - Windows Server 2016 (Server Core installation)
  - Windows Server 2016
  - Windows Server 2012 R2 (Server Core installation)
  - Windows Server 2012 R2
  - Windows Server 2012 (Server Core installation)
  - Windows Server 2012
  - Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
  - Windows Server 2008 R2 for x64-based Systems Service Pack 1
  - Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
  - Windows Server 2008 for x64-based Systems Service Pack 2
  - Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
  - Windows Server 2008 for 32-bit Systems Service Pack 2
  - Windows 11 Version 24H2 for x64-based Systems
  - Windows 11 Version 24H2 for ARM64-based Systems
  - Windows 11 Version 23H2 for x64-based Systems
  - Windows 11 Version 23H2 for ARM64-based Systems
  - Windows 11 Version 22H2 for x64-based Systems
  - Windows 11 Version 22H2 for ARM64-based Systems
  - Windows 10 Version 22H2 for x64-based Systems

    - Windows 10 Version 22H2 for ARM64-based Systems
    - Windows 10 Version 22H2 for 32-bit Systems
    - Windows 10 Version 21H2 for x64-based Systems
    - Windows 10 Version 21H2 for ARM64-based Systems
    - Windows 10 Version 21H2 for 32-bit Systems
    - Windows 10 Version 1809 for x64-based Systems
    - Windows 10 Version 1809 for 32-bit Systems
    - Windows 10 Version 1607 for x64-based Systems
    - Windows 10 Version 1607 for 32-bit Systems
    - Windows 10 for x64-based Systems
    - Windows 10 for 32-bit Systems
- Recommended Measures:
    - The official source has released a fix update for the vulnerability; please refer to the official instructions for update at the following URL: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073
- References:
    1. https://nvd.nist.gov/vuln/detail/CVE-2025-33073
    2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2025-33073
    3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073
    4. https://www.vicarius.io/vsociety/posts/cve-2025-33073-mitigation-script-improper-access-control-in-windows-smb-affects-microsoft-products

---

Computer and Communications Center
Network Systems Group