CERT-EU

Security Advisory 2024-077

Vulnerabilities in Microsoft Office

August 12, 2024 — v1.0

TLP:CLEAR

History:

- *12/08/2024 — v1.0 – Initial publication*

Summary

On August 8, 2024, Microsoft disclosed a high-severity vulnerability tracked as **CVE-2024-38200** affecting Office 2016 that could expose NTLM hashes to a remote attacker. This security flaw is caused by an information disclosure weakness that enables unauthorised actors to access protected information [1].

Technical Details

The vulnerability **CVE-2024-38200** (CVSS score: 7.5) is an information disclosure vulnerability that allows remote attackers to access NTLM hashes. Attackers can exploit this flaw via a specially crafted file or web-based attack, potentially leading to NTLM relay attacks or password cracking.

Affected Products

According to Microsoft's advisory, the following products are affected [4]:

- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2016 (32-bit edition)
- Microsoft Office LTSC 2021 for 32-bit editions
- Microsoft Office LTSC 2021 for 64-bit editions
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft Office 2019 for 64-bit editions
- Microsoft Office 2019 for 32-bit editions

Mitigations

1. Set the “Restrict NTLM: Outgoing NTLM traffic to remote servers” group policy to block NTLM traffic from computers running Windows 7, Windows Server 2008, or later to any remote server [2].
2. Add users to the Protected Users Security Group, which restricts NTLM as an authentication method [3].
3. Block all outbound traffic on TCP port 445 to prevent NTLM traffic from leaving the network.

Recommendations

CERT-EU recommends applying the mitigations provided by Microsoft [4], including blocking outbound NTLM traffic, while Microsoft releases the updates.

References

[1] https://www.bleepingcomputer.com/news/security/microsoft-discloses-unpatched-office-flaw-that-exposes-ntlm-hashes/

[2] https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-outgoing-ntlm-traffic-to-remote-servers#policy-management

[3] https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200