10 years CERT-EU

Security Advisory 2025-002

Multiple Vulnerabilities in Microsoft Products

2025-01-15 — v1.0

TLP:CLEAR

History:

- *15/01/2025 — v1.0 – Initial publication*

Summary

On January 14, Microsoft has released its January 2025 Patch Tuesday updates, addressing a total of 159 security vulnerabilities across various products [1,2]. The patches include fixes for critical and important-severity issues that could allow attackers to gain unauthorised access, execute arbitrary code, or elevate privileges. Three vulnerabilities were already being exploited in attacks.

Technical Details

The eight (8) zero-day vulnerabilities resolved in this update are:

- **CVE-2025-21333**, **CVE-2025-21334**, **CVE-2025-21335**, all with a CVSS score of 7.8, are elevation of privilege vulnerabilities in Windows Hyper-V that were exploited in attacks to gain SYSTEM privileges on Windows devices.
- **CVE-2025-21275**, with a CVSS score of 7.8, is an elevation of privileges flaw in the Windows App Package Installer that could lead to SYSTEM privileges.
- **CVE-2025-21308**, with a CVSS score of 6.5, is a spoofing vulnerability in Windows Themes. An attacker could convince a user to load a malicious file onto a vulnerable system and then convince the user to manipulate the specially crafted file, but not necessarily click or open the malicious file. Manipulating the malicious file could allow an attacker exfiltrated NTLM hashes to a remote server.
- **CVE-2025-21186**, **CVE-2025-21366**, **CVE-2025-21395**, all with a CVSS score of 7.8, are three remote code execution vulnerabilities in Microsoft Access that could be exploited when opening specially crafted Microsoft Access documents.

Microsoft also released fixes for 12 critical vulnerabilities, including:

- **CVE-2025-21294**, with a CVSS score of 8.1, is a Remote Code Execution vulnerability in Microsoft Digest Authentication.
- **CVE-2025-21354**, **CVE-2025-21362**, all with a CVSS score of 8.4, are Remote Code Execution vulnerabilities in Microsoft Office Excel.
- **CVE-2025-21307**, with a CVSS score of 9.8, is a Remote Code Execution vulnerability in the Reliable Multicast Transport driver (RMCAST). An unauthenticated attacker could

exploit the vulnerability by sending specially crafted packets to a Windows Pragmatic General Multicast (PGM) open socket on the server, without any interaction from the user. This vulnerability is only exploitable only if there is a program listening on a Pragmatic General Multicast (PGM) port.

- **CVE-2025-21311**, with a CVSS score of 9.8, is an Elevation of Privilege vulnerability in Windows NTLM V1.
- **CVE-2025-21298**, with a CVSS score of 9.8, is a Remote Code Execution vulnerability is Windows OLE. Exploitation of the vulnerability might involve either a victim opening a specially crafted email with an affected version of Microsoft Outlook software, or a victim's Outlook application displaying a preview of a specially crafted email.
- **CVE-2025-21309**, **CVE-2025-21297**, all with a CVSS score of 8.1, are Remote Code Execution vulnerabilities in Windows Remote Desktop Services. An attacker could successfully exploit this vulnerability by connecting to a system with the Remote Desktop Gateway role, triggering the race condition to create a use-after-free scenario, and then leveraging this to execute arbitrary code.

Affected Products

These vulnerabilities affect Windows Operating Systems and applications. Please refer to the vendor advisory for an exhaustive list of affected products [2].

Recommendations

It is recommended applying security updates as soon as possible, prioritising vulnerabilities with high scores and publicly exposed assets.

Workarounds

Some workarounds are provided by the vendor:

- In general, but specifically for the vulnerability **CVE-2025-21308**, it is recommended disabling NTLM authentication (if possible), or enabling the "Restrict NTLM: Outgoing NTLM traffic to remote servers" policy.
- In, general, but specifically for the vulnerability **CVE-2025-21311**, it is recommended to set the `LmCompatabilityLvl` to its maximum value (5) for all machines. This will prevent the usage of the older NTLMv1 protocol, while still allowing NTLMv2 [3].
- In general, but specifically for **CVE-2025-21298**, Microsoft recommends users read email messages in plain text format. However, this will have an impact on the ability to read email messages in HTML format.

References

[1] https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2025-patch-tuesday-fixes-8-zero-days-159-flaws/

[2] https://msrc.microsoft.com/update-guide/releaseNote/2025-Jan

[3] https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-security-lan-manager-authentication-level