

Security Advisory 2025-009

Critical Vulnerabilities in Windows Remote Desktop Services

2025-03-14 — v1.0

TLP:CLEAR

History:

- 14/03/2025 — v1.0 – Initial publication

Summary

On March 13, Microsoft has released its March security update, addressing 57 vulnerabilities across its product range, including six critical flaws. Among the critical vulnerabilities are **CVE-2025-24035** and **CVE-2025-24045**, both Remote Code Execution (RCE) vulnerabilities in Windows Remote Desktop Services (RDS). Each vulnerability has been assigned a CVSSv3 score of 8.1 and is rated as critical [1].

It is recommended updating affected assets as soon as possible.

Technical Details

The vulnerability **CVE-2025-24035** is caused by sensitive data storage in improperly locked memory and **CVE-2025-24045** is a more complex vulnerability to exploit, requiring an attacker to win a race condition [1].

Successful exploitation of these vulnerabilities could allow an unauthorised attacker to execute code over a network [1].

Microsoft has addressed 57 vulnerabilities in its products as part of the March 2025 Patch Tuesday update [2].

Affected Products

The following products are affected by **CVE-2025-24035** [3]:

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

- Windows 10
- Windows 11

The following products are affected by **CVE-2025-24045** [4]:

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Recommendations

CERT-EU recommends updating the affected products as soon as possible to the latest version, prioritising Internet facing applications.

It is also recommended restricting network access to sensitive services to only trusted network sources.

References

[1] <https://cybersecuritynews.com/windows-remote-desktop-services-code-vulnerability/>

[2] <https://msrc.microsoft.com/update-guide/releaseNote/2025-Mar>

[3] <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24035>

[4] <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24045>