An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2501150150

NCSC Advisory

Critical Windows OLE Remote Code Execution Vulnerability - CVE-2025-21298

(CVSS: 9.8)

15th, January 2025

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2025-21298

Published: 2025-01-14

Vendor: Microsoft

CVSS Score[1]: 9.8

Products Affected

Product	Version
Windows 10 Version 1809	10.0.17763.0 < 10.0.17763.6775
Windows Server 2019	10.0.17763.0 < 10.0.17763.6775
Windows Server 2019 (Server Core installation)	10.0.17763.0 < 10.0.17763.6775
Windows Server 2022	10.0.20348.0 < 10.0.20348.3091
Windows 10 Version 21H2	10.0.19043.0 < 10.0.19044.5371
Windows 11 version 22H2	10.0.22621.0 < 10.0.22621.4751
Windows 10 Version 22H2	10.0.19045.0 < 10.0.19045.5371
Windows Server 2025 (Server Core installation)	10.0.26100.0 < 10.0.26100.2894
Windows 11 version 22H3	10.0.22631.0 < 10.0.22621.4751
Windows 11 Version 23H2	10.0.22631.0 < 10.0.22631.4751
Windows Server 2022, 23H2 Edition (Server Core installation)	10.0.25398.0 < 10.0.25398.1369
Windows 11 Version 24H2	10.0.26100.0 < 10.0.26100.2894
Windows Server 2025	10.0.26100.0 < 10.0.26100.2894
Windows 10 Version 1507	10.0.10240.0 < 10.0.10240.20890
Windows 10 Version 1607	10.0.14393.0 < 10.0.14393.7699
Windows Server 2016	10.0.14393.0 < 10.0.14393.7699

[1] https://www.first.org/cvss/v3.0/specification-document

Windows Server 2016 (Server Core installation)	10.0.14393.0 < 10.0.14393.7699
Windows Server 2008 Service Pack 2	6.0.6003.0 < 6.0.6003.23070
Windows Server 2008 Service Pack 2 (Server Core installation)	6.0.6003.0 < 6.0.6003.23070
Windows Server 2008 Service Pack 2	6.0.6003.0 < 6.0.6003.23070
Windows Server 2008 R2 Service Pack 1	6.1.7601.0 < 6.1.7601.27520
Windows Server 2008 R2 Service Pack 1 (Server Core installation)	6.1.7601.0 < 6.1.7601.27520
Windows Server 2012	6.2.9200.0 < 6.2.9200.25273
Windows Server 2012 (Server Core installation)	6.2.9200.0 < 6.2.9200.25273
Windows Server 2012 R2	6.3.9600.0 < 6.3.9600.22371
Windows Server 2012 R2 (Server Core installation)	6.3.9600.0 < 6.3.9600.22371

Impact

An attacker could exploit CVE-2025-21298 by sending a specially crafted email to a victim using an affected version of Microsoft Outlook. The attack could be triggered either by the victim opening the email or by Outlook displaying a preview, potentially allowing the attacker to execute remote code on the victim's machine.

Common Weakness Enumeration (CWE)[2]: CWE-416: Use After Free

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Microsoft.

- https://nvd.nist.gov/vuln/detail/CVE-2025-21298
- https://www.cve.org/CVERecord?id=CVE-2025-21298
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21298