CVE-2025-21298

Windows OLE Remote Code Execution Vulnerability

Vairav Advisory Report

Date: February 04, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

A critical security vulnerability, identified as CVE-2025-21298, has been discovered in the Windows operating system, affecting multiple versions. This vulnerability arises from a use-after-free flaw in Object Linking and Embedding (OLE), potentially allowing remote code execution. Exploitation of this vulnerability could allow an attacker to execute arbitrary code on the victim's machine via specially crafted emails. Microsoft has released a security update to address the issue and recommends users implement mitigations such as reading emails in plain text to reduce the risk.

VULNERABILITY DETAILS

CVE-2025-21298

- **Description:** A use-after-free vulnerability in OLE may allow remote code execution if a victim opens a specially crafted email in Microsoft Outlook or views the email in the preview pane.
- **Impact:** Remote code execution leading to unauthorized actions on the affected system.
- **CVSS Score:** 9.8 (Critical)

AFFECTED VERSIONS

Windows 10, Windows 11, Windows Server (various versions including 2025, 2022, 2021, and earlier)

EXPLOIT DETAILS

This vulnerability can be exploited through specially crafted emails containing malicious RTF (Rich Text Format) attachments. An attacker can send such emails to victims, and if they open the email or even preview it in Outlook, remote code execution could occur.

RECOMMENDED ACTIONS

- Users are strongly urged to apply the security updates provided by Microsoft to address this vulnerability.

- Read email messages in plain text format by configuring Microsoft Outlook to reduce the risk of exploitation.

- For guidance on configuring Outlook for plain text mode, refer to Microsoft's instructions on how to read email messages in plain text.

ADDITIONAL SECURITY MEASURES

- Avoid opening unsolicited emails or email attachments from unknown or untrusted sources, particularly those containing rich content or RTF attachments.

REFERENCES

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21298

https://github.com/ynwarcs/CVE-2025-21298?tab=readme-ov-file

https://www.cve.org/CVERecord?id=CVE-2025-21298

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Website: https://vairavtech.com