Microsoft Outlook Has a 'Severe' Vulnerability That Could Easily Spread Malware

Microsoft has just officially warned users about the existence of a vulnerability that could allow hackers to easily spread malware through the Outlook email application.

Microsoft has officially warned users about the existence of a vulnerability that could allow hackers to easily spread malware through the Outlook email application. The company has also released a patch for this user-after-free vulnerability (currently tracked as CVE-2025-21298), and urged users to apply it immediately.

The vulnerability, CVE-2025-21298, is rated as critical (9.8) and can cause the use of freed memory to corrupt valid data or remotely deliver malware. The flaw resides in the Object Linking and Embedding (OLED) feature of Windows, which allows users to embed and link to other documents and objects, such as adding Excel charts to Word documents. The vulnerability is also particularly dangerous because it allows users to be infected with malware when previewing specially crafted emails.

" *Exploitation of the vulnerability could occur if a victim opens a specially crafted email using an affected version of Microsoft Outlook software, or if the victim's Outlook application displays a preview of a specially crafted email. This could result in an attacker executing remote code on the victim's machine," Microsoft said in a security alert .*

If you can't apply the patch at this time, Microsoft recommends that you take steps like viewing your email on large LANs as plain text, and disabling or restricting NTLM traffic altogether.

What happens when you view your email in plain text? Basically, all the animations, images, and fonts are removed. Your email won't look as fancy in plain text, but it's necessary to avoid interruptions while you wait for the update to the new version of Outlook.