Microsoft Office Use-After-Free Vulnerabilities Allow Local Code Execution

TL;DR

Microsoft patched two memory handling vulnerabilities in Microsoft Office that allow code execution on a local system. An attacker can abuse malicious Office files, including through the Preview Pane, to run code without credentials.

There is no sign of active exploitation, but the number of affected Office versions means organizations should patch immediately.

Overview

Microsoft released security updates for two use-after-free vulnerabilities in Microsoft Office that affect both Windows and macOS systems. Tracked as CVE-2026-20952 and CVE-2026-20953 (CVSS 8.4), the flaws stem from improper memory handling and allow arbitrary code to run in the context of the logged-in user.

Microsoft rates the attack as local, but this is still an Office file problem, and a crafted document delivered through email or messaging is enough to trigger it. Microsoft also confirmed that the Preview Pane can be used as an attack vector, which reduces the amount of user interaction required and increases the chance of accidental exposure. There is no evidence of active exploitation at this time, but the low complexity of the flaws and lack of required privileges make them likely candidates for future phishing-based campaigns.

The vulnerabilities impact a broad set of Microsoft Office products, including Office 2016, Office 2019, Microsoft 365 Apps for Enterprise, and Office LTSC 2021 and 2024 on both Windows and macOS. Microsoft released fixes for all supported versions, and organizations should patch as soon as possible.

Aspire Protects

- **Patch** – Apply Microsoft's January 2026 security updates across all supported Office installations on Windows and macOS. See Microsoft's advisories for guidance (CVE-2026-20952 and CVE-2026-20953)
- Review email and messaging controls that allow Office attachments or links to reach users.
- Restrict or disable the Preview Pane in higher-risk environments where Office documents are frequently received from external sources.

- Monitor endpoint activity for unusual Office process behavior following document interaction.

TTPs

Initial Access

- Phishing [T1566] – The attacker may have delivered a crafted Office document through email or messaging to entice user interaction.

Execution

- User Execution: Malicious File [T1204.002] – The attacker may have relied on the user opening a malicious Office file or triggering it through the Preview Pane.

- Exploitation for Client Execution [T1203] – The attacker may have exploited the use-after-free condition in Microsoft Office to execute code in the context of the logged-in user.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

These Microsoft Office vulnerabilities affect any organization that relies on Office applications for daily business operations.

- Government
- Education
- Energy
- Healthcare
- Retail
- Finance
- Technology
- Legal
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CVE-2026-20952 - Security Update Guide - Microsoft - Microsoft Office Remote Code Execution Vulnerability
CVE-2026-20953 - Security Update Guide - Microsoft - Microsoft Office Remote Code Execution Vulnerability