Microsoft Fixes Six Actively Exploited Zero-Days

TL;DR

Microsoft's February 2026 Patch Tuesday addressed six zero-day vulnerabilities that are being exploited in the wild. The flaws span Windows Shell, MSHTML, Microsoft Word, Remote Desktop Services, Desktop Window Manager, and Windows Remote Access Connection Manager.

Several issues allow security feature bypass or local privilege escalation, creating opportunities for attackers to chain access and deepen compromise.

Overview

Microsoft released February 2026 Patch Tuesday updates fixing 58 vulnerabilities, including six zero-days that were already being exploited prior to patch availability. Three of these zero-days have also been publicly disclosed, increasing the likelihood of abuse.

The exploited issues largely center on bypassing built-in Windows and Office protections or escalating privileges after initial access. While some attacks require user interaction, others allow attackers who already have local access to elevate to SYSTEM-level privileges.

Microsoft has not publicly confirmed whether these vulnerabilities were used together in a single campaign.

- **CVE-2026-21510** (CVSS pending) – Windows Shell Security Feature Bypass
  Allows attackers to bypass Windows SmartScreen and shell security prompts by tricking a user into opening a crafted shortcut or link, likely bypassing Mark-of-the-Web protections.
- **CVE-2026-21513** (CVSS pending) – MSHTML Framework Security Feature Bypass
  A protection mechanism failure in MSHTML that allows attackers to bypass security controls over a network. Exploitation details have not been released.
- **CVE-2026-21514** (CVSS pending) – Microsoft Word Security Feature Bypass
  Bypasses OLE mitigations in Microsoft Office, allowing malicious Office documents to execute content without expected protections. The Preview Pane is not an attack vector.
- **CVE-2026-21519** (CVSS pending) – Desktop Window Manager Elevation of Privilege
  Allows local attackers to escalate privileges to SYSTEM, significantly increasing post-compromise impact.

- **CVE-2026-21525** (CVSS pending) – Windows Remote Access Connection Manager Denial of Service
  A null pointer dereference that allows attackers to crash the service locally. While not a data-theft flaw, it has been observed in active exploitation.
- **CVE-2026-21533** (CVSS pending) – Windows Remote Desktop Services Elevation of Privilege
  Improper privilege management allows authenticated users to elevate privileges locally.

These zero-days focus on bypassing protections users rely on to stay safe and escalating access once attackers are already inside. Several flaws only need one bad click or a foothold on a single endpoint to turn into SYSTEM-level control. Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch** – Apply February 2026 Microsoft security updates immediately across all supported systems. See Microsoft's advisories for more information.
  - CVE-2026-21533
  - CVE-2026-21525
  - CVE-2026-21519
  - CVE-2026-21514
  - CVE-2026-21513
  - CVE-2026-21510
- Treat user-triggered exploit alerts as high-priority events, even when no malware is immediately visible.
- Monitor for suspicious shortcut files, Office document execution chains, and abnormal privilege escalation activity.
- Review endpoint protection alerts tied to Windows Shell, MSHTML, Word, and Remote Desktop Services.

TTPs to Watch

Initial Access

- User Execution [T1204] – The attacker may have relied on malicious links, shortcut files, or Office documents that required user interaction to trigger exploitation.

Defense Evasion

- Subvert Trust Controls [T1553] – The attacker may have bypassed built-in Windows and Office security warnings such as SmartScreen and OLE protections.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may have escalated local privileges to SYSTEM through Desktop Window Manager or Remote Desktop Services flaws.

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 vulnerabilities affect any organization running Microsoft Windows or Office products, particularly environments where endpoint hardening and user awareness controls are inconsistent.

- Finance
- Government
- Education
- Energy
- Healthcare
- Retail
- Technology
- 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-2026-21510 - Security Update Guide - Microsoft - Windows Shell Security Feature Bypass Vulnerability

CVE-2026-21513 - Security Update Guide - Microsoft - MSHTML Framework Security Feature Bypass Vulnerability

CVE-2026-21514 - Security Update Guide - Microsoft - Microsoft Word Security Feature Bypass Vulnerability

CVE-2026-21519 - Security Update Guide - Microsoft - Desktop Window Manager Elevation of Privilege Vulnerability

CVE-2026-21525 - Security Update Guide - Microsoft - Windows Remote Access Connection Manager Denial of Service Vulnerability

Security Update Guide - Loading - Microsoft