EnCyb

Severity: Critical

Advisory Type: Vulnerability

Microsoft Patch Tuesday Advisory

FEBRUARY- 2026

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Microsoft's February 2026 Patch Tuesday fixes 54 vulnerabilities, including six actively exploited zero-days affecting Windows, Office, Exchange, and Azure. Immediate patching is critical, as attackers are leveraging security bypass and privilege escalation flaws to gain SYSTEM-level control and compromise enterprise environments.

- Active Region: Global
- Affected Sector: Enterprise IT, Cloud Infrastructure, Government, and Endpoints
- Affected Product: Microsoft Windows, Microsoft Office (Word/Outlook/Excel), Microsoft Exchange Server, Azure Services, GitHub Copilot, Visual Studio Code
- Severity: Critical(2), High(50), Medium(2)

CVE LIST

CVE	Severity	Description
CVE-2026-23655	Critical	Microsoft ACI Confidential Containers Information Disclosure
CVE-2026-21522	Critical	Microsoft ACI Confidential Containers Elevation of Privilege
CVE-2026-21537	High	Microsoft Defender for Endpoint Linux Extension Remote Code Execution
CVE-2026-21533	High	Windows Remote Desktop Services Elevation of Privilege
CVE-2026-21531	High	Azure SDK Remote Code Execution
CVE-2026-21529	High	Azure HDInsight Spoofing
CVE-2026-21528	High	Azure IoT Explorer Information Disclosure
CVE-2026-21527	High	Microsoft Exchange Server Spoofing
CVE-2026-21523	High	GitHub Copilot & Visual Studio Code Remote Code Execution
CVE-2026-21519	High	Desktop Window Manager Elevation of Privilege
CVE-2026-21518	High	GitHub Copilot & VS Code Security Feature Bypass
CVE-2026-21517	High	Windows App for Mac Installer Elevation of Privilege
CVE-2026-21516	High	GitHub Copilot for JetBrains Remote Code Execution
CVE-2026-21514	High	Microsoft Word Security Feature Bypass
CVE-2026-21513	High	MSHTML Framework Security Feature Bypass
CVE-2026-21512	High	Azure DevOps Server Cross-Site Scripting
CVE-2026-21511	High	Microsoft Outlook Spoofing
CVE-2026-21510	High	Windows Shell Security Feature Bypass
CVE-2026-21508	High	Windows Storage Elevation of Privilege
CVE-2026-21261	High	Microsoft Excel Information Disclosure
CVE-2026-21260	High	Microsoft Outlook Spoofing
CVE-2026-21259	High	Microsoft Excel Elevation of Privilege
CVE-2026-21258	High	Microsoft Excel Information Disclosure
CVE-2026-21257	High	GitHub Copilot & Visual Studio Elevation of Privilege
CVE-2026-21256	High	GitHub Copilot & Visual Studio Remote Code Execution
CVE-2026-21255	High	Windows Hyper-V Security Feature Bypass

CVE-2026-21253	High	Mailslot File System Elevation of Privilege
CVE-2026-21251	High	Cluster Client Failover Elevation of Privilege
CVE-2026-21250	High	Windows HTTP.sys Elevation of Privilege
CVE-2026-21222	High	Windows Kernel Information Disclosure
CVE-2026-21248	High	Windows Hyper-V Remote Code Execution
CVE-2026-21247	High	Windows Hyper-V Remote Code Execution
CVE-2026-21246	High	Windows Graphics Component Elevation of Privilege
CVE-2026-21245	High	Windows Kernel Elevation of Privilege
CVE-2026-21244	High	Windows Hyper-V Remote Code Execution
CVE-2026-21243	High	Windows LDAP Denial of Service
CVE-2026-21242	High	Windows Subsystem for Linux Elevation of Privilege
CVE-2026-21241	High	Windows Ancillary Function Driver Elevation of Privilege
CVE-2026-21240	High	Windows HTTP.sys Elevation of Privilege
CVE-2026-21239	High	Windows Kernel Elevation of Privilege
CVE-2026-21238	High	Windows Ancillary Function Driver Elevation of Privilege
CVE-2026-21237	High	Windows Subsystem for Linux Elevation of Privilege
CVE-2026-21236	High	Windows Ancillary Function Driver Elevation of Privilege
CVE-2026-21235	High	Windows Graphics Component Elevation of Privilege
CVE-2026-21234	High	Windows Connected Devices Platform Service Elevation of Privilege
CVE-2026-21232	High	Windows HTTP.sys Elevation of Privilege
CVE-2026-21231	High	Windows Kernel Elevation of Privilege
CVE-2026-21229	High	Power BI Remote Code Execution
CVE-2026-21228	High	Azure Local Remote Code Execution
CVE-2026-21218	High	.NET Spoofing
CVE-2026-20846	High	GDI+ Denial of Service
CVE-2026-20841	High	Windows Notepad Remote Code Execution
CVE-2026-21525	Medium	Windows Remote Access Connection Manager Denial of Service
CVE-2026-21249	Medium	Windows NTLM Spoofing

TECHNICAL DETAILS – ZERO DAY VULNERABILITY

CVE-2026-21510 – Windows Shell Security Feature Bypass

• **Attack Vector:** User interaction with a specially crafted file downloaded from the internet (e.g., shortcut, archive, or document).

• **Cause:** Improper enforcement of Mark of the Web (MoTW) security checks allows bypass of trust validation mechanisms.

• **Prerequisite:** Victim must open or interact with a malicious file delivered via phishing, web download, or network share.

• **Risk:** Enables attackers to bypass Windows security warnings and execute malicious payloads without standard user prompts, often used as an initial access vector in exploit chains.

CVE-2026-21513 – MSHTML Framework Security Feature Bypass

- **Attack Vector:** User opens a malicious file or web content leveraging the MSHTML rendering engine.
- **Cause:** Inadequate security prompt enforcement in MSHTML allows bypass of protection mechanisms.
- **Prerequisite:** User interaction with crafted content (e.g., malicious document or HTML-based payload).
- **Risk:** Allows execution of attacker-controlled content without proper security warnings, facilitating follow-on exploitation such as privilege escalation.

CVE-2026-21514 – Microsoft Word Security Feature Bypass

- **Attack Vector:** Opening a specially crafted Microsoft Word document.
- **Cause:** Improper enforcement of OLE mitigation protections within Word.
- **Prerequisite:** Victim opens a malicious Office document delivered via phishing or shared location.
- **Risk:** Bypasses built-in Office defences, enabling embedded malicious objects or payload execution that can be chained with other exploits.

CVE-2026-21519 – Desktop Window Manager Elevation of Privilege

- **Attack Vector:** Local interaction with Desktop Window Manager through crafted window objects.
- **Cause:** Type confusion vulnerability in DWM memory handling.
- **Prerequisite:** Attacker must have local code execution on the target system.
- **Risk:** Allows elevation to SYSTEM privileges, enabling full control of the affected machine and facilitating lateral movement.

CVE-2026-21533 – Windows Remote Desktop Services Elevation of Privilege

- **Attack Vector:** Authenticated interaction with Windows Remote Desktop Services.

• **Cause:** Improper privilege management allowing escalation within RDS components.

• **Prerequisite:** Valid authenticated user access to the system.

• **Risk:** Enables attackers to escalate privileges to SYSTEM level, compromising remote-access infrastructure and enterprise servers.

CVE-2026-21525 – Windows Remote Access Connection Manager Denial of Service

• **Attack Vector:** Local exploitation via crafted input targeting the Remote Access Connection Manager service.

• **Cause:** Null pointer dereferences leading to service crash.

• **Prerequisite:** Ability to trigger the vulnerable service locally.

• **Risk:** Causes VPN or remote access service crashes, potentially disrupting enterprise connectivity and remote workforce operations.

RECOMMENDATIONS

- Patch all systems immediately
- Prioritize internet-facing servers
- Enforce least privilege (remove local admin)
- Enable ASR rules in Defender
- Restrict and secure RDP with MFA

REFERENCE

Consider referring link below for detailed information on vulnerabilities.

- https://msrc.microsoft.com/update-guide/releaseNote/2026-Feb

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com