مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Microsoft February 2026 Patch Tuesday Security Updates

Tracking #:432318385

Date:11-02-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft released its February 2026 Patch Tuesday security update, addressing 61 vulnerabilities across its product ecosystem. This release is particularly critical as it includes six zero-day vulnerabilities that are actively being exploited in the wild.

TECHNICAL DETAILS:

Microsoft released its February 2026 Patch Tuesday security update, addressing 61 vulnerabilities across its product ecosystem. This release is particularly critical as it includes six zero-day vulnerabilities that are actively being exploited in the wild.

Key Highlights:

- **6 zero-day vulnerabilities** actively exploited in the wild
- **5 critical-severity vulnerabilities** requiring immediate attention
- Affected products include Windows Desktop Manager, Remote Desktop Services, Azure services, Microsoft Office, and core Windows components
- Multiple privilege escalation vulnerabilities enabling attackers to gain SYSTEM-level access
- Security feature bypass flaws affecting Windows Shell, MSHTML Framework, and Microsoft Word

Detailed Vulnerability List

Actively Exploited Zero-Day Vulnerabilities (CRITICAL PRIORITY)

CVE ID	Description	Status
CVE-2026-21519	Desktop Window Manager Elevation of Privilege - Type confusion flaw allowing authenticated attackers to gain SYSTEM privileges	Exploited in Wild
CVE-2026-21533	Windows Remote Desktop Services Elevation of Privilege - Improper privilege management enabling SYSTEM-level access	Exploited in Wild
CVE-2026-21510	Windows Shell Security Feature Bypass - Protection mechanism failure allowing network security feature bypass via malicious links/shortcuts	Exploited in Wild
CVE-2026-21514	Microsoft Word Security Feature Bypass - Allows attackers to bypass Protected View through malicious Office files	Exploited in Wild
CVE-2026-21525	Windows Remote Access Connection Manager Denial of Service - Null pointer dereference causing VPN/dial-up service disruption	Exploited in Wild
CVE-2026-21513	MSHTML Framework Security Feature Bypass - Enables bypassing security features when rendering HTML in Windows applications	Exploited in Wild

Critical-Severity Vulnerabilities

CVE ID	Description
CVE-2026-24300	Azure Front Door Elevation of Privilege
CVE-2026-21522	Microsoft ACI Confidential Containers Elevation of Privilege - Command

	injection allowing arbitrary code execution in container context
CVE-2026-23655	Microsoft ACI Confidential Containers Information Disclosure - Allows disclosure of secret tokens and cryptographic keys
CVE-2026-24302	Azure Arc Elevation of Privilege
CVE-2026-21532	Azure Function Information Disclosure

High-Priority Important-Severity Vulnerabilities

CVE ID	Description
CVE-2026-21511	Microsoft Outlook Spoofing - Deserialization vulnerability enabling email spoofing and BEC attacks
CVE-2026-21253	Mailslot File System Elevation of Privilege - Allows escalation to SYSTEM privileges
CVE-2026-21241	Windows Ancillary Function Driver for WinSock Elevation of Privilege - Enables SYSTEM-level access
CVE-2026-21238	Windows Ancillary Function Driver for WinSock Elevation of Privilege - Second vulnerability enabling SYSTEM access
CVE-2026-21231	Windows Kernel Elevation of Privilege - Kernel vulnerability allowing SYSTEM privilege escalation

RECOMMENDATIONS:

- Prioritize remediation of Zero-Day vulnerabilities and Deploy February 2026 cumulative updates across all affected products.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://msrc.microsoft.com/update-guide/releaseNote/2025-Feb