Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's February 2026 Patch Tuesday Fixes Active Zero-Day Exploits

Date of Publication	Admiralty Code	TA Number
February 11, 2026	A1	TA2026042

Summary

First Seen: February 10, 2026
Affected Platforms: Microsoft Notepad App, Windows Kernel, Windows Remote Desktop, Microsoft Office, Microsoft Exchange Server, Google Chromium and more
Impact: Information Disclosure, Denial of Service, Remote Code Execution, Elevation of Privilege, Security Feature Bypass, Spoofing

Exploitable CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-21510	Windows Shell Security Feature Bypass Vulnerability	Windows Shell	✓	✓	✓
CVE-2026-21513	MSHTML Framework Security Feature Bypass Vulnerability	MSHTML Framework	✓	✓	✓
CVE-2026-21514	Microsoft Word Security Feature Bypass Vulnerability	Microsoft Office Word	✓	✓	✓
CVE-2026-21519	Desktop Window Manager Elevation of Privilege Vulnerability	Desktop Window Manager	✓	✓	✓
CVE-2026-21525	Windows Remote Access Connection Manager Denial of Service Vulnerability	Windows Remote Access Connection Manager	✓	✓	✓
CVE-2026-21533	Windows Remote Desktop Services Elevation of Privilege Vulnerability	Windows Remote Desktop	✓	✓	✓

Note: The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-21231	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	✗	✗	✓
CVE-2026-21238	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	✗	✗	✓
CVE-2026-21241	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	✗	✗	✓
CVE-2026-21253	Mailslot File System Elevation of Privilege Vulnerability	Mailslot File System	✗	✗	✓
CVE-2026-21511	Microsoft Outlook Spoofing Vulnerability	Microsoft Office Outlook	✗	✗	✓
CVE-2026-21522	Microsoft ACI Confidential Containers Elevation of Privilege Vulnerability	Azure Compute Gallery	✗	✗	✓
CVE-2026-21532	Azure Function Information Disclosure Vulnerability	Azure Function	✗	✗	✓
CVE-2026-23655	Microsoft ACI Confidential Containers Information Disclosure Vulnerability	Azure Compute Gallery	✗	✗	✓
CVE-2026-24300	Azure Front Door Elevation of Privilege Vulnerability	Azure Front Door (AFD)	✗	✗	✓
CVE-2026-24302	Azure Arc Elevation of Privilege Vulnerability	Azure Arc	✗	✗	✓

Note: The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1189: Drive-by Compromise	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
Execution	T1059: Command and Scripting Interpreter	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
Defense Evasion	T1036: Masquerading	
	T1218: System Binary Proxy Execution	
	T1553: Subvert Trust Controls	T1553.005: Mark-of-the-Web Bypass
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1543: Create or Modify System Process	T1543.003: Windows Service
Credential Access	T1552: Unsecured Credentials	
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
Impact	T1499: Endpoint Denial of Service	

Vulnerability Details

#1

Microsoft's February 2026 Patch Tuesday delivers a substantial set of security updates, addressing 59 vulnerabilities across its product ecosystem. Of these, 5 are rated Critical, 52 Important, and 2 Moderate. The vulnerabilities span multiple impact categories, including 12 Remote Code Execution (RCE), 25 Elevation of Privilege (EoP), 6 Information Disclosure, 3 Denial of Service (DoS), 5 Security Feature Bypass, and 8 Spoofing flaws.

#2

Microsoft also resolved one non-Microsoft Chromium-based vulnerability, bringing the total number of CVEs addressed this month to 60. Notably, 16 CVEs are assessed as either actively exploited or at increased risk of exploitation, underscoring the urgency of rapid patch deployment. Of greatest concern, six vulnerabilities were actively exploited in the wild at the time of release, three of which had been publicly disclosed prior to patching.

#3

The six zero-days span several attack surfaces and exploitation stages. CVE-2026-21510 (Windows Shell) and CVE-2026-21513 (MSHTML Framework) are security feature bypass vulnerabilities that can be exploited by convincing users to open malicious links, shortcut files, or specially crafted HTML content.

#4

CVE-2026-21510 enables attackers to bypass Windows SmartScreen, Windows Shell and related security warnings, while CVE-2026-21513 allows adversaries to circumvent MSHTML protections and achieve code execution when a victim opens a malicious HTML or LNK file. CVE-2026-21514 affects Microsoft Word, bypassing OLE mitigations designed to restrict unsafe COM/OLE control execution, and requires user interaction via a crafted Office document.

#5

Privilege escalation vulnerabilities form another critical component of this month's zero-days. CVE-2026-21519 in the Desktop Window Manager and CVE-2026-21533 in Windows Remote Desktop Services both allow local attackers to escalate privileges to SYSTEM level after gaining initial access. Such flaws are particularly valuable in post-compromise scenarios, enabling further exploitation across the environment. The sixth zero-day, CVE-2026-21525, is a denial-of-service vulnerability in the Windows Remote Access Connection Manager that can disrupt system availability. Notably, this is the only moderate-severity flaw among the six actively exploited vulnerabilities.

#6

Beyond the zero-days, Microsoft patched two critical vulnerabilities in Azure ACI Confidential Containers. CVE-2026-21522 is a command injection issue that could allow privilege escalation within containerized workloads, while CVE-2026-23655 is an information disclosure vulnerability that may expose sensitive tokens or cryptographic keys.

#7

A spoofing vulnerability in Microsoft Outlook (CVE-2026-21511) is also notable, as it can be triggered via crafted emails and leverages the preview pane as an attack vector. Additionally, Microsoft addressed RCE-related issues affecting GitHub Copilot integrations within developer environments, including Visual Studio, VS Code, and JetBrains products, stemming from prompt injection risks in Copilot agent workflows.

#8

This release also introduces phased updates to replace expiring Secure Boot certificates originally issued in 2011, reinforcing platform trust and boot integrity. Given the volume of elevation-of-privilege flaws and the presence of multiple actively exploited zero-days, organizations should prioritize patch deployment, particularly for internet-facing systems, remote access infrastructure, and endpoints exposed to user-supplied content such as email attachments and web-based documents. Accelerated testing and rollout are strongly recommended to mitigate exploitation risk.

Recommendations

Conduct an extensive service exposure evaluation to identify any vulnerable services that may be publicly accessible. Take immediate and decisive action to address any identified vulnerabilities, either by installing essential **patches** or adopting security measures.

Keep your systems up to date by implementing the most recent security updates. To avoid the introduction of new vulnerabilities, follow security rules adapted to unique devices. Furthermore, to strengthen the resilience of devices and apps exposed to the internet, thoroughly review their configurations.

Prioritize patching the actively exploited vulnerabilities CVE-2026-21510, CVE-2026-21513, CVE-2026-21514, CVE-2026-21519, CVE-2026-21525, CVE-2026-21533. These vulnerabilities pose significant exploitation risks and should be addressed urgently.

Implement network segmentation to restrict unauthorized access and reduce the impact of potential attacks. This can be especially effective in scenarios where network adjacency is a factor.

Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

All CVEs

CVE	NAME	PRODUCT	IMPACT
CVE-2023-2804	Libjpeg-turbo Heap Based Overflow Vulnerability	Windows Win32K - GRFX	Remote Code Execution
CVE-2026-0391	Microsoft Edge (Chromium-based) for Android Spoofing Vulnerability	Microsoft Edge for Android	Spoofing
CVE-2026-20841	Windows Notepad App Remote Code Execution Vulnerability	Windows Notepad App	Remote Code Execution
CVE-2026-20846	GDI+ Denial of Service Vulnerability	Windows GDI+	Denial of Service
CVE-2026-21218	.NET Spoofing Vulnerability	.NET	Spoofing
CVE-2026-21222	Windows Kernel Information Disclosure Vulnerability	Windows Kernel	Information Disclosure
CVE-2026-21228	Azure Local Remote Code Execution Vulnerability	Azure Local	Remote Code Execution
CVE-2026-21229	Power BI Remote Code Execution Vulnerability	Power BI	Remote Code Execution
CVE-2026-21231	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-21232	Windows HTTP.sys Elevation of Privilege Vulnerability	Windows HTTP.sys	Elevation of Privilege
CVE-2026-21234	Windows Connected Devices Platform Service Elevation of Privilege Vulnerability	Windows Connected Devices Platform Service	Elevation of Privilege
CVE-2026-21235	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Graphics Component	Elevation of Privilege
CVE-2026-21236	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-21237	Windows Subsystem for Linux Elevation of Privilege Vulnerability	Windows Subsystem for Linux	Elevation of Privilege
CVE-2026-21238	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-21239	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2026-21240	Windows HTTP.sys Elevation of Privilege Vulnerability	Windows HTTP.sys	Elevation of Privilege
CVE-2026-21241	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-21242	Windows Subsystem for Linux Elevation of Privilege Vulnerability	Windows Subsystem for Linux	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-21243	Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability	Windows LDAP - Lightweight Directory Access Protocol	Denial of Service
CVE-2026-21244	Windows Hyper-V Remote Code Execution Vulnerability	Role: Windows Hyper-V	Remote Code Execution
CVE-2026-21245	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2026-21246	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Graphics Component	Elevation of Privilege
CVE-2026-21247	Windows Hyper-V Remote Code Execution Vulnerability	Role: Windows Hyper-V	Remote Code Execution
CVE-2026-21248	Windows Hyper-V Remote Code Execution Vulnerability	Role: Windows Hyper-V	Remote Code Execution
CVE-2026-21249	Windows NTLM Spoofing Vulnerability	Windows NTLM	Spoofing
CVE-2026-21250	Windows HTTP.sys Elevation of Privilege Vulnerability	Windows HTTP.sys	Elevation of Privilege
CVE-2026-21251	Cluster Client Failover (CCF) Elevation of Privilege Vulnerability	Windows Cluster Client Failover	Elevation of Privilege
CVE-2026-21253	Mailslot File System Elevation of Privilege Vulnerability	Mailslot File System	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-21255	Windows Hyper-V Security Feature Bypass Vulnerability	Role: Windows Hyper-V	Security Feature Bypass
CVE-2026-21256	GitHub Copilot and Visual Studio Remote Code Execution Vulnerability	GitHub Copilot and Visual Studio	Remote Code Execution
CVE-2026-21257	GitHub Copilot and Visual Studio Elevation of Privilege Vulnerability	GitHub Copilot and Visual Studio	Elevation of Privilege
CVE-2026-21258	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure
CVE-2026-21259	Microsoft Excel Elevation of Privilege Vulnerability	Microsoft Office Excel	Elevation of Privilege
CVE-2026-21260	Microsoft Outlook Spoofing Vulnerability	Microsoft Office Outlook	Spoofing
CVE-2026-21261	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure
CVE-2026-21508	Windows Storage Elevation of Privilege Vulnerability	Windows Storage	Elevation of Privilege
CVE-2026-21510	Windows Shell Security Feature Bypass Vulnerability	Windows Shell	Security Feature Bypass
CVE-2026-21511	Microsoft Outlook Spoofing Vulnerability	Microsoft Office Outlook	Spoofing

CVE	NAME	PRODUCT	IMPACT
CVE-2026-21512	Azure DevOps Server Cross-Site Scripting Vulnerability	Azure DevOps Server	Spoofing
CVE-2026-21513	MSHTML Framework Security Feature Bypass Vulnerability	MSHTML Framework	Security Feature Bypass
CVE-2026-21514	Microsoft Word Security Feature Bypass Vulnerability	Microsoft Office Word	Security Feature Bypass
CVE-2026-21516	GitHub Copilot for Jetbrains Remote Code Execution Vulnerability	Github Copilot	Remote Code Execution
CVE-2026-21517	Windows App for Mac Installer Elevation of Privilege Vulnerability	Windows App for Mac	Elevation of Privilege
CVE-2026-21518	GitHub Copilot and Visual Studio Code Security Feature Bypass Vulnerability	GitHub Copilot and Visual Studio Code	Security Feature Bypass
CVE-2026-21519	Desktop Window Manager Elevation of Privilege Vulnerability	Desktop Window Manager	Elevation of Privilege
CVE-2026-21522	Microsoft ACI Confidential Containers Elevation of Privilege Vulnerability	Azure Compute Gallery	Elevation of Privilege
CVE-2026-21523	GitHub Copilot and Visual Studio Code Remote Code Execution Vulnerability	GitHub Copilot and Visual Studio	Remote Code Execution
CVE-2026-21525	Windows Remote Access Connection Manager Denial of Service Vulnerability	Windows Remote Access Connection Manager	Denial of Service

CVE	NAME	PRODUCT	IMPACT
CVE-2026-21527	Microsoft Exchange Server Spoofing Vulnerability	Microsoft Exchange Server	Spoofing
CVE-2026-21528	Azure IoT Explorer Information Disclosure Vulnerability	Azure IoT SDK	Information Disclosure
CVE-2026-21529	Azure HDInsight Spoofing Vulnerability	Azure HDInsights	Spoofing
CVE-2026-21531	Azure SDK for Python Remote Code Execution Vulnerability	Azure SDK	Remote Code Execution
CVE-2026-21532	Azure Function Information Disclosure Vulnerability	Azure Function	Information Disclosure
CVE-2026-21533	Windows Remote Desktop Services Elevation of Privilege Vulnerability	Windows Remote Desktop	Elevation of Privilege
CVE-2026-21537	Microsoft Defender for Endpoint Linux Extension Remote Code Execution Vulnerability	Microsoft Defender for Linux	Remote Code Execution
CVE-2026-23655	Microsoft ACI Confidential Containers Information Disclosure Vulnerability	Azure Compute Gallery	Information Disclosure
CVE-2026-24300	Azure Front Door Elevation of Privilege Vulnerability	Azure Front Door (AFD)	Elevation of Privilege
CVE-2026-24302	Azure Arc Elevation of Privilege Vulnerability	Azure Arc	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-1861	Chromium Heap Buffer Overflow in libvpx Vulnerability	Microsoft Edge (Chromium-based)	Application Crash

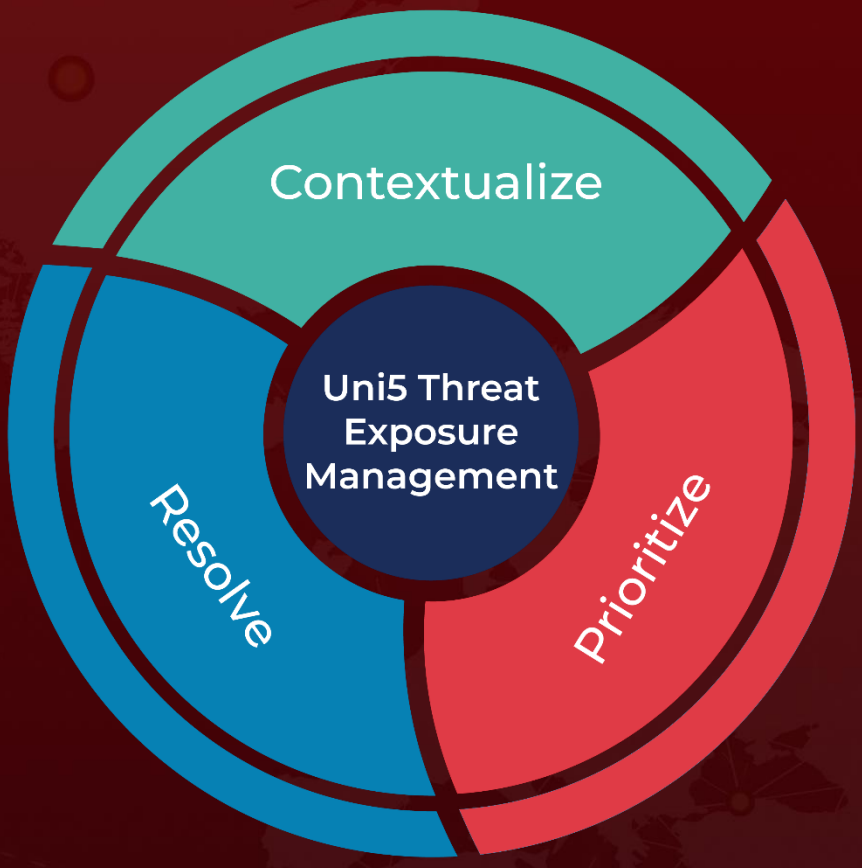
References

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 11, 2026 • 11:00 PM

More at www.hivepro.com