Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's January 2026 Patch Tuesday

Date of Publication	Admiralty Code	TA Number
January 14, 2026	A1	TA2026013

Summary

First Seen: January 13, 2026
Affected Platforms: Microsoft Windows, Windows Kerberos, Windows NTFS, Windows Management Services, Windows Deployment Services, SQL Server, Microsoft Office SharePoint, Microsoft Office, Google Chromium, and more
Impact: Information Disclosure, Denial of Service, Remote Code Execution, Elevation of Privilege, Security Feature Bypass, Spoofing, Tampering

Exploitable CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-20805	Microsoft Windows Information Disclosure Vulnerability	Windows 10 - 11 25H2, Windows Server 2012, 2016, 2019, 2025, 2022	✓	✓	✓
CVE-2026-21265	Secure Boot Certificate Expiration Security Feature Bypass Vulnerability	Windows 10 - 11 25H2, Windows Server 2012, 2016, 2025, 2022, 2019	✗	✗	✓
CVE-2026-20816	Windows Installer Elevation of Privilege Vulnerability	Windows 10 - 11 25H2, Windows Server 2012, 2008, 2016, 2025, 2022, 2019	✗	✗	✓
CVE-2026-20817	Windows Error Reporting Service Elevation of Privilege Vulnerability	Windows 10 - 11 25H2, Windows Server 2025, 2022	✗	✗	✓
CVE-2026-20820	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows 10 - 11 25H2, Windows Server 2012, 2008, 2016, 2025, 2022, 2019	✗	✗	✓
CVE-2026-20840	Windows NTFS Remote Code Execution Vulnerability	Windows 10 - 11 25H2, Windows Server 2022, 2025, 2012, 2016, 2008, 2019	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-20843	Windows Routing and Remote Access Service (RRAS) Elevation of Privilege Vulnerability	Windows 10 - 11 25H2, Windows Server 2012, 2008, 2016, 2025, 2022, 2019	✗	✗	✓
CVE-2026-20860	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows 10 - 11 25H2, Windows Server 2012, 2008, 2016, 2025, 2022, 2019	✗	✗	✓
CVE-2026-20871	Desktop Windows Manager Elevation of Privilege Vulnerability	Windows 10 - 11 25H2, Windows Server 2025, 2022	✗	✗	✓
CVE-2026-20922	Windows NTFS Remote Code Execution Vulnerability	Windows 10 - 11 25H2, Windows Server 2012, 2008, 2016, 2025, 2022, 2019	✗	✗	✓
CVE-2023-31096	Windows Agere Soft Modem Driver Elevation of Privilege Vulnerability	Windows 10 - 11 25H2, Windows Server 2012, 2008, 2016, 2025, 2022, 2019	✗	✗	✓
CVE-2026-0628	Chromium Insufficient policy enforcement in WebView tag Vulnerability	Microsoft Edge (Chromium-based)	✗	✗	✓

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

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0007** Discovery	**TA0010** Exfiltration
TA0011 Command and Control	**TA0040** Impact	**T1566** Phishing	**T1204** User Execution
T1059 Command and Scripting Interpreter	**T1068** Exploitation for Privilege Escalation	**T1553** Subvert Trust Controls	**T1082** System Information Discovery
T1547 Boot or Logon Autostart Execution	**T1499** Endpoint Denial of Service	**T1195** Supply Chain Compromise	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1071** Application Layer Protocol		

Vulnerability Details

#1

Microsoft's January 2026 Patch Tuesday marks one of the more substantial security releases in recent months, delivering fixes for 112 vulnerabilities across its product ecosystem. Of these, eight are rated critical, while the remaining 104 are classified as important. The addressed flaws span a broad range of vulnerability classes, including 22 remote code execution issues, 55 elevation of privilege flaws, 22 information disclosure bugs, two denial-of-service vulnerabilities, three security feature bypasses, five spoofing issues, and three tampering weaknesses. In addition to Microsoft-owned products, patches were also issued for three non-Microsoft CVEs, bringing the total number of resolved vulnerabilities this month to 115. Particularly concerning is the fact that 12 of these CVEs are assessed as being at risk of active exploitation, reinforcing the need for rapid and prioritized patch deployment.

#2

The zero-day vulnerability addressed in this cycle, CVE-2026-20805, stands out. This flaw affects the Desktop Window Manager and enables local information disclosure by exposing sensitive data to an unauthorized actor, provided the attacker already has authorized access.

#3

CVE-2026-21265, on the other hand, impacts Windows Secure Boot and represents a security feature bypass resulting from the expiration of Microsoft certificates stored in the UEFI Key Exchange Key (KEK) and signature database (DB). Systems running affected certificate versions must be updated to maintain Secure Boot protections and avoid the loss of critical security assurances tied to the Windows boot process.

#4

Several high-impact elevation of privilege vulnerabilities were also resolved in this release. CVE-2026-20816 affects the Windows Installer and could allow an attacker to escalate privileges to SYSTEM. CVE-2026-20817 targets the Windows Error Reporting Service and similarly enables an authenticated attacker to obtain SYSTEM-level access. CVE-2026-20820 resides in the Windows Common Log File System driver, where a heap-based buffer overflow could be exploited to achieve full privilege escalation. These flaws are particularly dangerous in post-compromise scenarios, as they allow attackers to move from limited access to complete system control.

#5

Remote code execution risks were addressed as well, notably CVE-2026-20840 and CVE-2026-20922, both of which affect the Windows NTFS subsystem. Exploitation of these heap-based buffer overflow vulnerabilities could enable authenticated attackers to execute arbitrary code, potentially leading to full system compromise. Additional elevation of privilege issues were fixed in the Windows Ancillary Function Driver for WinSock (CVE-2026-20860), where a type confusion flaw could grant SYSTEM privileges, and in the Windows Routing and Remote Access Service (CVE-2026-20843), which also allows attackers to elevate their access to the highest privilege level.

#6

Beyond the Windows ecosystem, Microsoft included fixes for Chromium-based vulnerabilities, most notably CVE-2026-0628. This issue stems from insufficient policy enforcement in the WebView tag in Google Chrome prior to version 143.0.7499.192. An attacker who persuaded a user to install a malicious browser extension could exploit this weakness to inject scripts or HTML into privileged pages, effectively breaching browser security boundaries.

#7

Finally, Microsoft addressed a long-standing third-party driver risk with CVE-2023-31096, which affects the Agere Soft Modem drivers that ship natively with supported Windows versions. Due to elevation of privilege concerns associated with these drivers, Microsoft has removed the affected agrsm64.sys and agrsm.sys files entirely as part of the January 2026 cumulative update, eliminating the vulnerable components from supported systems.

#8

Taken together, Microsoft's January 2026 security updates underscore the continuing evolution and complexity of the modern threat landscape. With multiple zero-day issues, privilege escalation flaws, and remote code execution vulnerabilities addressed in a single release, organizations are strongly advised to deploy these patches as a matter of priority to reduce exposure and defend against both opportunistic attacks and more sophisticated, targeted campaigns.

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-2026-20805, CVE-2026-21265, and CVE-2023-31096. 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-2026-0386	Windows Deployment Services Remote Code Execution Vulnerability	Windows Deployment Services	Remote Code Execution
CVE-2026-20803	Microsoft SQL Server Elevation of Privilege Vulnerability	SQL Server	Elevation of Privilege
CVE-2026-20804	Windows Hello Tampering Vulnerability	Windows Hello	Tampering
CVE-2026-20805	Microsoft Windows Information Disclosure Vulnerability	Desktop Window Manager	Information Disclosure
CVE-2026-20808	Windows File Explorer Elevation of Privilege Vulnerability	Printer Association Object	Elevation of Privilege
CVE-2026-20809	Windows Kernel Memory Elevation of Privilege Vulnerability	Windows Kernel Memory	Elevation of Privilege
CVE-2026-20810	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-20811	Win32k Elevation of Privilege Vulnerability	Windows Win32K - ICOMP	Elevation of Privilege
CVE-2026-20812	LDAP Tampering Vulnerability	Windows LDAP - Lightweight Directory Access Protocol	Tampering

CVE	NAME	PRODUCT	IMPACT
CVE-2026-20814	DirectX Graphics Kernel Elevation of Privilege Vulnerability	Graphics Kernel	Elevation of Privilege
CVE-2026-20815	Capability Access Management Service (camsvc) Elevation of Privilege Vulnerability	Capability Access Management Service (camsvc)	Elevation of Privilege
CVE-2026-20816	Windows Installer Elevation of Privilege Vulnerability	Windows Installer	Elevation of Privilege
CVE-2026-20817	Windows Error Reporting Service Elevation of Privilege Vulnerability	Windows Error Reporting	Elevation of Privilege
CVE-2026-20818	Windows Kernel Information Disclosure Vulnerability	Windows Kernel	Information Disclosure
CVE-2026-20819	Windows Virtualization-Based Security (VBS) Information Disclosure Vulnerability	Windows Virtualization-Based Security (VBS) Enclave	Information Disclosure
CVE-2026-20820	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows Common Log File System Driver	Elevation of Privilege
CVE-2026-20821	Remote Procedure Call Information Disclosure Vulnerability	Windows Remote Procedure Call	Information Disclosure
CVE-2026-20822	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Graphics Component	Elevation of Privilege
CVE-2026-20823	Windows File Explorer Information Disclosure Vulnerability	Windows File Explorer	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2026-20824	Windows Remote Assistance Security Feature Bypass Vulnerability	Windows Remote Assistance	Security Feature Bypass
CVE-2026-20825	Windows Hyper-V Information Disclosure Vulnerability	Windows Hyper-V	Information Disclosure
CVE-2026-20826	Tablet Windows User Interface (TWINUI) Subsystem Information Disclosure Vulnerability	Tablet Windows User Interface (TWINUI) Subsystem	Elevation of Privilege
CVE-2026-20827	Tablet Windows User Interface (TWINUI) Subsystem Information Disclosure Vulnerability	Tablet Windows User Interface (TWINUI) Subsystem	Information Disclosure
CVE-2026-20828	Windows rndismp6.sys Information Disclosure Vulnerability	Windows Internet Connection Sharing (ICS)	Information Disclosure
CVE-2026-20829	TPM Trustlet Information Disclosure Vulnerability	Windows TPM	Information Disclosure
CVE-2026-20830	Capability Access Management Service (camsvc) Elevation of Privilege Vulnerability	Capability Access Management Service (camsvc)	Elevation of Privilege
CVE-2026-20831	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-20832	Windows Remote Procedure Call Interface Definition Language (IDL) Elevation of Privilege Vulnerability	Windows Remote Procedure Call Interface Definition Language (IDL)	Elevation of Privilege
CVE-2026-20833	Windows Kerberos Information Disclosure Vulnerability	Windows Kerberos	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2026-20834	Windows Spoofing Vulnerability	Windows Shell	Spoofing
CVE-2026-20835	Capability Access Management Service (camsvc) Information Disclosure Vulnerability	Capability Access Management Service (camsvc)	Information Disclosure
CVE-2026-20836	DirectX Graphics Kernel Elevation of Privilege Vulnerability	Graphics Kernel	Elevation of Privilege
CVE-2026-20837	Windows Media Remote Code Execution Vulnerability	Windows Media	Remote Code Execution
CVE-2026-20838	Windows Kernel Information Disclosure Vulnerability	Windows Kernel	Information Disclosure
CVE-2026-20839	Windows Client-Side Caching (CSC) Service Information Disclosure Vulnerability	Windows Client-Side Caching (CSC) Service	Information Disclosure
CVE-2026-20840	Windows NTFS Remote Code Execution Vulnerability	Windows NTFS	Remote Code Execution
CVE-2026-20842	Microsoft DWM Core Library Elevation of Privilege Vulnerability	Windows DWM	Elevation of Privilege
CVE-2026-20843	Windows Routing and Remote Access Service (RRAS) Elevation of Privilege Vulnerability	Windows Routing and Remote Access Service (RRAS)	Elevation of Privilege
CVE-2026-20844	Windows Clipboard Server Elevation of Privilege Vulnerability	Windows Clipboard Server	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-20847	Microsoft Windows File Explorer Spoofing Vulnerability	Windows Shell	Spoofing
CVE-2026-20848	Windows SMB Server Elevation of Privilege Vulnerability	Windows SMB Server	Elevation of Privilege
CVE-2026-20849	Windows Kerberos Elevation of Privilege Vulnerability	Windows Kerberos	Elevation of Privilege
CVE-2026-20851	Capability Access Management Service (camsvc) Information Disclosure Vulnerability	Capability Access Management Service (camsvc)	Information Disclosure
CVE-2026-20852	Windows Hello Tampering Vulnerability	Windows Hello	Tampering
CVE-2026-20853	Windows WalletService Elevation of Privilege Vulnerability	Windows WalletService	Elevation of Privilege
CVE-2026-20854	Windows Local Security Authority Subsystem Service (LSASS) Remote Code Execution Vulnerability	Windows Local Security Authority Subsystem Service (LSASS)	Remote Code Execution
CVE-2026-20856	Windows Server Update Service (WSUS) Remote Code Execution Vulnerability	Windows Server Update Service	Remote Code Execution
CVE-2026-20857	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Cloud Files Mini Filter Driver	Elevation of Privilege
CVE-2026-20858	Windows Management Services Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-20859	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	Windows Kernel-Mode Drivers	Elevation of Privilege
CVE-2026-20860	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-20861	Windows Management Services Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege
CVE-2026-20862	Windows Management Services Information Disclosure Vulnerability	Windows Management Services	Information Disclosure
CVE-2026-20863	Win32k Elevation of Privilege Vulnerability	Windows Win32K - ICOMP	Elevation of Privilege
CVE-2026-20864	Windows Connected Devices Platform Service Elevation of Privilege Vulnerability	Connected Devices Platform Service (Cdpsvc)	Elevation of Privilege
CVE-2026-20865	Windows Management Services Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege
CVE-2026-20866	Windows Management Services Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege
CVE-2026-20867	Windows Management Services Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege
CVE-2026-20868	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-20869	Windows Local Session Manager (LSM) Elevation of Privilege Vulnerability	Windows Local Session Manager (LSM)	Elevation of Privilege
CVE-2026-20870	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Windows Win32K - ICOMP	Elevation of Privilege
CVE-2026-20871	Desktop Windows Manager Elevation of Privilege Vulnerability	Desktop Window Manager	Elevation of Privilege
CVE-2026-20872	NTLM Hash Disclosure Spoofing Vulnerability	Windows NTLM	Spoofing
CVE-2026-20873	Windows Management Services Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege
CVE-2026-20874	Windows Management Services Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege
CVE-2026-20875	Windows Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability	Windows Local Security Authority Subsystem Service (LSASS)	Denial of Service
CVE-2026-20876	Windows Virtualization-Based Security (VBS) Enclave Elevation of Privilege Vulnerability	Windows Virtualization-Based Security (VBS) Enclave	Elevation of Privilege
CVE-2026-20877	Windows Management Services Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege
CVE-2026-20918	Windows Management Services Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-20919	Windows SMB Server Elevation of Privilege Vulnerability	Windows SMB Server	Elevation of Privilege
CVE-2026-20920	Win32k Elevation of Privilege Vulnerability	Windows Win32K - ICOMP	Elevation of Privilege
CVE-2026-20921	Windows SMB Server Elevation of Privilege Vulnerability	Windows SMB Server	Elevation of Privilege
CVE-2026-20922	Windows NTFS Remote Code Execution Vulnerability	Windows NTFS	Remote Code Execution
CVE-2026-20923	Windows Management Services Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege
CVE-2026-20924	Windows Management Services Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege
CVE-2026-20925	NTLM Hash Disclosure Spoofing Vulnerability	Windows NTLM	Spoofing
CVE-2026-20926	Windows SMB Server Elevation of Privilege Vulnerability	Windows SMB Server	Elevation of Privilege
CVE-2026-20927	Windows SMB Server Denial of Service Vulnerability	Windows SMB Server	Denial of Service
CVE-2026-20929	Windows HTTP.sys Elevation of Privilege Vulnerability	Windows HTTP.sys	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-20931	Windows Telephony Service Elevation of Privilege Vulnerability	Windows Telephony Service	Elevation of Privilege
CVE-2026-20932	Windows File Explorer Information Disclosure Vulnerability	Windows File Explorer	Information Disclosure
CVE-2026-20934	Windows SMB Server Elevation of Privilege Vulnerability	Windows SMB Server	Elevation of Privilege
CVE-2026-20935	Windows Virtualization-Based Security (VBS) Information Disclosure Vulnerability	Windows Virtualization-Based Security (VBS) Enclave	Information Disclosure
CVE-2026-20936	Windows NDIS Information Disclosure Vulnerability	Windows NDIS	Information Disclosure
CVE-2026-20937	Windows File Explorer Information Disclosure Vulnerability	Windows File Explorer	Information Disclosure
CVE-2026-20938	Windows Virtualization-Based Security (VBS) Enclave Elevation of Privilege Vulnerability	Windows Virtualization-Based Security (VBS) Enclave	Elevation of Privilege
CVE-2026-20939	Windows File Explorer Information Disclosure Vulnerability	Windows File Explorer	Information Disclosure
CVE-2026-20940	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Cloud Files Mini Filter Driver	Elevation of Privilege
CVE-2026-20941	Host Process for Windows Tasks Elevation of Privilege Vulnerability	Host Process for Windows Tasks	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-20943	Microsoft Office Click-To-Run Elevation of Privilege Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-20944	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution
CVE-2026-20946	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-20947	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-20948	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution
CVE-2026-20949	Microsoft Excel Security Feature Bypass Vulnerability	Microsoft Office Excel	Security Feature Bypass
CVE-2026-20950	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-20951	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-20952	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-20953	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-20955	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-20956	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-20957	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-20958	Microsoft SharePoint Information Disclosure Vulnerability	Microsoft Office SharePoint	Information Disclosure
CVE-2026-20959	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-20962	Dynamic Root of Trust for Measurement (DRTM) Information Disclosure Vulnerability	Dynamic Root of Trust for Measurement (DRTM)	Information Disclosure
CVE-2026-20963	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-20965	Windows Admin Center Elevation of Privilege Vulnerability	Windows Admin Center	Elevation of Privilege
CVE-2026-21219	Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability	Inbox COM Objects	Remote Code Execution
CVE-2026-21221	Capability Access Management Service (camsvc) Elevation of Privilege Vulnerability	Capability Access Management Service (camsvc)	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-21224	Azure Connected Machine Agent Elevation of Privilege Vulnerability	Azure Connected Machine Agent	Elevation of Privilege
CVE-2026-21226	Azure Core shared client library for Python Remote Code Execution Vulnerability	Azure Core shared client library for Python	Remote Code Execution
CVE-2026-21265	Secure Boot Certificate Expiration Security Feature Bypass Vulnerability	Windows Secure Boot	Security Feature Bypass
CVE-2023-31096	Windows Agere Soft Modem Driver Elevation of Privilege Vulnerability	Agere Windows Modem Driver	Elevation of Privilege
CVE-2024-55414	Windows Motorola Soft Modem Driver Elevation of Privilege Vulnerability	Windows Motorola Soft Modem Driver	Elevation of Privilege
CVE-2026-0628	Chromium Insufficient policy enforcement in WebView tag Vulnerability	Microsoft Edge (Chromium-based)	Bypass Security

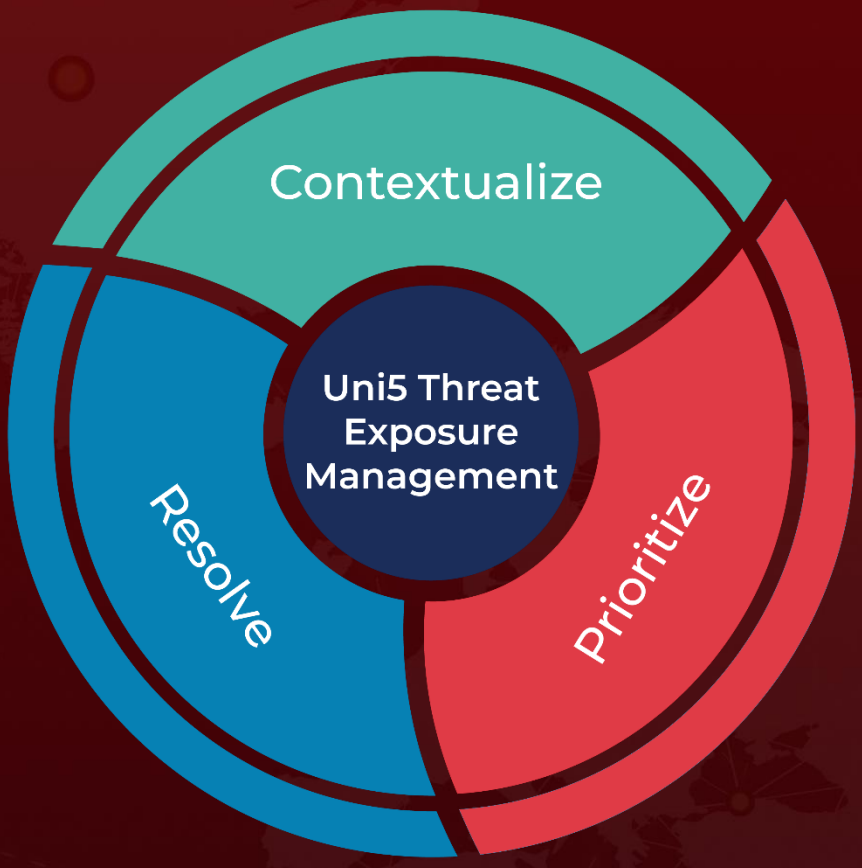
References

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

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

January 14, 2026 . 8:30 AM

More at www.hivepro.com