Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's June 2026 Patch Tuesday

Date of Publication	Admiralty Code	TA Number
June 10, 2026	A1	TA2026162

Summary

First Seen: June 10, 2026
Affected Products: Microsoft Windows HTTP Protocol Stack (HTTP.sys), Windows Collaborative Translation Framework (CTFMON), Windows BitLocker (Windows 11 and Windows Server 2022/2025 using TPM-only protection), Windows NT OS Kernel, Microsoft Windows Remote Desktop Client, Microsoft Graphics Component, Windows Win32K GRFX (graphics subsystem), Winlogon, Microsoft SharePoint Server, Windows NTLM, and Windows DWM Core Library
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-2026-49160	HTTP.sys Denial of Service Vulnerability	Windows 11 Version 23H2, 10 Version 22H2; Windows Server 2025, 2022, 2019, 2016	✗	✗	✓
CVE-2026-45586	Windows Collaborative Translation Framework (CTFMON) Elevation of Privilege Vulnerability	Windows Server 2012 R2, 2019, 2016 (Server Core installation), 2025; Windows 10 Version 1607; Windows 11 Version 26H1 for ARM64-based Systems	✗	✗	✓
CVE-2026-50507	Windows BitLocker Security Feature Bypass Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025; Windows 10 Version 1607; Windows 11 Version 26H1	✗	✗	✓
CVE-2026-42980	NT OS Kernel Elevation of Privilege Vulnerability	Windows Server 2025; Windows 10 Version 1607; Windows 11 Version 24H2	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-42985	Remote Desktop Client Remote Code Execution Vulnerability	Windows Server 2012, 2016, 2019, 2022, ; Windows 10 Version 1607; Windows 11 Version 26H1, Windows App Client for Windows Desktop	✗	✗	✓
CVE-2026-42986	Microsoft Graphics Component Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025; Windows 11 Version 24H2; Windows 10 Version 1607	✗	✗	✓
CVE-2026-42989	Winlogon Elevation of Privilege Vulnerability	Windows Server 2012, 2016, ,2019 , 2022, 2025; Windows 10 Version 1607; Windows 11 Version 26H1	✗	✗	✓
CVE-2026-44803	Windows Graphics Component Remote Code Execution Vulnerability	Windows 10 Version 1607; Windows 11 version 26H1; Windows Server 2025, 2012, 2016, 2022, 2019; Microsoft Word for Android; Microsoft PowerPoint for Android	✗	✗	✓
CVE-2026-44812	Windows Graphics Component Remote Code Execution Vulnerability	Microsoft PowerPoint for Android, Microsoft Excel for Android, Windows Server 2012, 2016, 2022, 2019, 2025; Windows 10 Version 1607; Windows 11 Version 26H1	✗	✗	✓
CVE-2026-45481	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft SharePoint Server Subscription Edition; Microsoft SharePoint Server 2019; Microsoft SharePoint Enterprise Server 2016	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-45658	Windows BitLocker Security Feature Bypass Vulnerability	Windows Server 2012, 2016, 2025, 2022, 2019; Windows 10 Version 1607; Windows 11 Version 26H1	✗	✗	✓
CVE-2026-47291	HTTP.sys Remote Code Execution Vulnerability	Windows Server 2012, 2016, 2025, 2022, 2019; Windows 10 Version 1607; Windows 11 Version 26H1; Windows 10 Version 22H2	✗	✗	✓
CVE-2026-47634	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft SharePoint Server Subscription Edition; Microsoft SharePoint Server 2019	✗	✗	✓
CVE-2026-50508	Windows NTLM Spoofing Vulnerability	Windows Server 2012, 2016, 2004, 2022; Windows 10 Version 1607; Windows 11 Version 22H2	✗	✗	✓
CVE-2026-42905	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows 10 Version 21H2; Windows Server 2022, 2019, 2025, 2016, 2012; Windows 10 Version 22H2; Windows 11 Version 26H1	✗	✗	✓

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

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1189: Drive-by Compromise	
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
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	
	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	T1499.004: Application or System Exploitation

Vulnerability Details

#1

Microsoft’s June 2026 Patch Tuesday delivers an extensive batch of security updates, addressing 204 vulnerabilities across its product ecosystem. Beyond its own products, Microsoft also released patches for 2 non-Microsoft CVEs, pushing the total count of vulnerabilities addressed this month to 206. These include 39 rated critical and 167 marked important in severity. The vulnerabilities span various categories: 65 Elevation of Privilege, 55 Remote Code Execution (RCE), 30 Information Disclosure, 27 Spoofing, 19 Security Feature Bypass, 7 Denial of Service, and 3 Tampering issues. Notably, 15 of these CVEs are considered at risk of active exploitation, underscoring the urgency of prompt patch deployment.

#2

The most dangerous flaw is CVE-2026-47291, a remote code execution bug in the Windows HTTP Protocol Stack (HTTP.sys) caused by an integer overflow. An unauthenticated attacker can trigger it with a single crafted packet, putting any internet-facing service built on HTTP.sys at risk. The same component carries CVE-2026-49160, a publicly disclosed zero-day denial-of-service that maps to the "HTTP/2 Bomb" technique: a trivial amount of data forces the server to reserve huge blocks of memory and hold them open through flow-control tricks. Testing reportedly drained 64 GB of RAM from an IIS server in about 45 seconds. Microsoft's fix adds a "MaxHeadersCount" registry setting that caps headers in HTTP/2 and HTTP/3 requests.

#3

The Windows graphics stack carries a second cluster of critical RCEs. CVE-2026-44803 and CVE-2026-44812 both stem from an integer overflow in the Win32K GRFX subsystem and let an attacker run code locally; Microsoft rates both "more likely" to be exploited. CVE-2026-42985 is a network-exploitable RCE in the Windows Remote Desktop Client (heap-based buffer overflow, CWE-122) typically a malicious RDP server to run code on any victim who connects.

#4

Several "more likely" privilege-escalation flaws give an attacker with a foothold a clean path to SYSTEM: CVE-2026-42980 (NT OS Kernel), CVE-2026-42986 (Graphics Component), CVE-2026-42989 (Winlogon), and CVE-2026-42905 (DWM Core Library). CVE-2026-45586, a publicly disclosed zero-day, escalates privileges in the Collaborative Translation Framework (CTFMON) via link following; it matches the public "GreenPlasma" exploit, which can spawn a SYSTEM shell.

#5

Two BitLocker bypasses round out the high-impact set. CVE-2026-50507 (CVSS 6.8), the publicly disclosed third zero-day, is a protection-mechanism failure letting an attacker with physical access defeat BitLocker with the "YellowKey" exploit, which uses crafted files on USB/EFI media plus the Recovery Environment to open a shell over encrypted drives. It mainly affects TPM-only setups on Windows 11 and Server 2022/2025; TPM+PIN was Microsoft's earlier interim mitigation. CVE-2026-45658 is a second BitLocker bypass in the same release.

#6

Finally, three spoofing flaws: CVE-2026-45481 and CVE-2026-47634 in SharePoint Server (both "more likely"), and CVE-2026-50508 in Windows NTLM. The sources give no exploitation chains, but such flaws typically enable content forgery, credential relay, or social engineering. As of the release date, none of the three publicly disclosed zero-days are known to be exploited.

Recommendations

Apply the June 2026 Security Updates Immediately: Deploy the June 9, 2026 Microsoft security updates across all affected Windows clients, servers, Remote Desktop clients, and SharePoint Server instances without delay. These updates remediate all fifteen vulnerabilities in this advisory, including the three publicly disclosed zero-days and the CVSS 9.8 HTTP.sys remote code execution flaw. Patching is the single most effective control, given that functional proof-of-concept code is already public for several issues.

Prioritize Internet-Facing and Network-Reachable Systems: Treat servers running IIS or any service built on the Windows HTTP Protocol Stack (HTTP.sys) as top-priority patch targets for CVE-2026-47291 and CVE-2026-49160, since both are reachable over the network with little or no authentication. Where immediate patching is not possible for the HTTP/2 denial-of-service issue, apply Microsoft's new "MaxHeadersCount" registry setting to limit the number of headers accepted in HTTP/2 and HTTP/3 requests as an interim mitigation.

Harden BitLocker-Protected Endpoints: For devices relying on TPM-only BitLocker protection, particularly Windows 11 and Windows Server 2022/2025, apply the fixes for CVE-2026-50507 and CVE-2026-45658, and consider enabling TPM+PIN authentication to raise the bar against physical-access attacks such as the publicly disclosed "YellowKey" technique. Enforce boot-environment and recovery-environment controls to prevent untrusted USB or EFI media from subverting encryption.

Constrain Privilege-Escalation Exposure: Because CVE-2026-42980, CVE-2026-42985, CVE-2026-42986, CVE-2026-42989, CVE-2026-45586, and CVE-2026-42905 enable an attacker with an initial foothold to elevate to higher privileges (often SYSTEM), enforce least privilege, restrict local administrative rights, and monitor for anomalous process creation, unexpected SYSTEM-level shells, and Remote Desktop connections to untrusted servers until patching is complete.

All CVEs

CVE	NAME	PRODUCT	IMPACT
CVE-2026-26142	Nuance PowerScribe Remote Code Execution Vulnerability	Nuance PowerScribe	Remote Code Execution
CVE-2026-32193	Azure Kubernetes Service (AKS) Remote Code Execution Vulnerability	Microsoft Azure Kubernetes Service	Remote Code Execution
CVE-2026-33113	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-33828	Windows Device Health Attestation (DHA) Elevation of Privilege Vulnerability	Microsoft Azure Attestation service and Device Health Attestation Service	Elevation of Privilege
CVE-2026-34335	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-40371	Microsoft Dynamics 365 (on-premises) Elevation of Privilege Vulnerability	Microsoft Dynamics 365 (on-premises)	Elevation of Privilege
CVE-2026-40376	Visual Studio Code Elevation of Privilege Vulnerability	Visual Studio Code	Elevation of Privilege
CVE-2026-40404	Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability	Windows Universal Disk Format File System Driver (UDFS)	Elevation of Privilege
CVE-2026-40409	Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability	Windows Universal Disk Format File System Driver (UDFS)	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-41092	Microsoft Kinect Elevation of Privilege Vulnerability	Microsoft Kinect	Elevation of Privilege
CVE-2026-41098	Azure Stack Edge Spoofing Vulnerability	Azure Stack Edge	Spoofing
CVE-2026-41108	Windows DNS Client Elevation of Privilege Vulnerability	Microsoft Windows DNS	Elevation of Privilege
CVE-2026-42824	M365 Copilot Information Disclosure Vulnerability	M365 Copilot	Information Disclosure
CVE-2026-42828	Windows Projected File System Elevation of Privilege Vulnerability	Windows Projected File System Filter Driver	Elevation of Privilege
CVE-2026-42829	Windows Administrator Protection Secure Feature Bypass Vulnerability	Windows Administrator Protection	Security Feature Bypass
CVE-2026-42835	Microsoft Teams for Android Information Disclosure Vulnerability	Microsoft Teams for Android	Information Disclosure
CVE-2026-42836	Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability	Function Discovery Service (fdwsd.dll)	Elevation of Privilege
CVE-2026-42837	Windows Projected File System Elevation of Privilege Vulnerability	Windows Projected File System Filter Driver	Elevation of Privilege
CVE-2026-42902	Microsoft PowerToys Elevation of Privilege Vulnerability	Microsoft PowerToys	Elevation of Privilege
CVE-2026-42903	Windows Kerberos Denial of Service Vulnerability	Windows Kerberos	Denial of Service

CVE	NAME	PRODUCT	IMPACT
CVE-2026-42904	Windows TCP/IP Elevation of Privilege Vulnerability	Windows TCP/IP	Elevation of Privilege
CVE-2026-42905	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege
CVE-2026-42906	Windows Shell Information Disclosure Vulnerability	Windows Shell	Information Disclosure
CVE-2026-42907	Windows Shell Information Disclosure Vulnerability	Windows Shell	Information Disclosure
CVE-2026-42908	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability	Windows RDP	Information Disclosure
CVE-2026-42909	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2026-42910	Windows Hotpatch Monitoring Service Elevation of Privilege Vulnerability	Windows Hotpatch Monitoring Service	Elevation of Privilege
CVE-2026-42911	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-42912	Windows Telephony Service Elevation of Privilege Vulnerability	Windows Telephony Service	Elevation of Privilege
CVE-2026-42913	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2026-42914	Windows Kerberos Denial of Service Vulnerability	Windows Kerberos	Denial of Service

CVE	NAME	PRODUCT	IMPACT
CVE-2026-42915	Windows TCP/IP Denial of Service Vulnerability	Windows TCP/IP	Denial of Service
CVE-2026-42916	NT OS Kernel Elevation of Privilege Vulnerability	Windows NT OS Kernel	Elevation of Privilege
CVE-2026-42968	Windows Telephony Server Information Disclosure Vulnerability	Windows Telephony Service	Information Disclosure
CVE-2026-42969	Windows Push Notification Information Disclosure Vulnerability	Windows Push Notifications	Information Disclosure
CVE-2026-42970	Windows Push Notification Information Disclosure Vulnerability	Windows Push Notifications	Information Disclosure
CVE-2026-42971	Windows Push Notification Information Disclosure Vulnerability	Windows Push Notifications	Information Disclosure
CVE-2026-42972	Windows Hyper-V Information Disclosure Vulnerability	Role: Windows Hyper-V	Information Disclosure
CVE-2026-42973	Windows Push Notification Information Disclosure Vulnerability	Windows Push Notifications	Information Disclosure
CVE-2026-42974	Windows Performance Monitor Remote Code Execution Vulnerability	Windows Performance Monitor	Remote Code Execution
CVE-2026-42977	Windows Push Notifications Elevation of Privilege Vulnerability	Windows Push Notifications	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-42978	Windows Push Notifications Elevation of Privilege Vulnerability	Windows Push Notifications	Elevation of Privilege
CVE-2026-42979	Windows Push Notifications Elevation of Privilege Vulnerability	Windows Push Notifications	Elevation of Privilege
CVE-2026-42980	NT OS Kernel Elevation of Privilege Vulnerability	Windows NT OS Kernel	Elevation of Privilege
CVE-2026-42981	Windows Performance Monitor Remote Code Execution Vulnerability	Windows Performance Monitor	Remote Code Execution
CVE-2026-42983	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege
CVE-2026-42984	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2026-42985	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2026-42986	Microsoft Graphics Component Elevation of Privilege Vulnerability	Microsoft Graphics Component	Elevation of Privilege
CVE-2026-42987	Windows Deployment Services (WDS) Remote Code Execution	Windows Deployment Services	Remote Code Execution
CVE-2026-42989	Winlogon Elevation of Privilege Vulnerability	Winlogon	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-42991	Windows Push Notifications Elevation of Privilege Vulnerability	Windows Push Notifications	Elevation of Privilege
CVE-2026-42992	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2026-42993	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2026-44799	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2026-44801	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2026-44802	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege
CVE-2026-44803	Windows Graphics Component Remote Code Execution Vulnerability	Windows Win32K - GRFX	Remote Code Execution
CVE-2026-44804	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege
CVE-2026-44805	Windows Network Controller (NC) Host Agent Denial of Service Vulnerability	Windows Network Controller (NC) Host Agent	Denial of Service
CVE-2026-44807	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-44808	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege
CVE-2026-44809	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows Common Log File System Driver	Elevation of Privilege
CVE-2026-44810	Microsoft Cryptographic Services Elevation of Privilege Vulnerability	Windows Cryptographic Services	Elevation of Privilege
CVE-2026-44811	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege
CVE-2026-44812	Windows Graphics Component Remote Code Execution Vulnerability	Windows Win32K - GRFX	Remote Code Execution
CVE-2026-44813	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege
CVE-2026-44814	Windows DWM Core Library Information Disclosure Vulnerability	Windows DWM Core Library	Information Disclosure
CVE-2026-44815	DHCP Client Service Remote Code Execution Vulnerability	Windows DHCP Client	Remote Code Execution
CVE-2026-44817	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-44818	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-44819	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-44820	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-44821	Microsoft Office Information Disclosure Vulnerability	Microsoft Office	Information Disclosure
CVE-2026-44822	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure
CVE-2026-44823	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-44824	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-45453	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-45454	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-45455	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure
CVE-2026-45456	Microsoft Outlook and Word Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-45457	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-45458	Microsoft Outlook and Word Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-45459	Microsoft Excel Security Feature Bypass Vulnerability	Microsoft Office Excel	Security Feature Bypass
CVE-2026-45460	Microsoft Office Information Disclosure Vulnerability	Microsoft Office	Information Disclosure
CVE-2026-45461	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-45462	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-45463	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-45464	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-45465	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing

CVE	NAME	PRODUCT	IMPACT
CVE-2026-45466	Microsoft Word Information Disclosure Vulnerability	Microsoft Office Word	Information Disclosure
CVE-2026-45467	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-45468	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-45469	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-45471	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution
CVE-2026-45472	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-45474	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-45475	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-45476	Microsoft Azure Network Adapter Elevation of Privilege Vulnerability	Linux MANA Driver	Elevation of Privilege
CVE-2026-45479	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing

CVE	NAME	PRODUCT	IMPACT
CVE-2026-45481	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-45482	Microsoft Visual Studio Code CoPilot Chat Extension Security Feature Bypass Vulnerability	GitHub Copilot and Visual Studio Code	Security Feature Bypass
CVE-2026-45483	Microsoft Office Project Server Spoofing Vulnerability	Microsoft Office Project	Spoofing
CVE-2026-45484	Microsoft SharePoint Elevation of Privilege Vulnerability	Microsoft Office SharePoint	Elevation of Privilege
CVE-2026-45485	Microsoft Office Information Disclosure Vulnerability	Microsoft Office	Information Disclosure
CVE-2026-45486	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution
CVE-2026-45487	Windows Program Compatibility Assistant Service Elevation of Privilege Vulnerability	Windows Program Compatibility Assistant Service	Elevation of Privilege
CVE-2026-45490	.NET SDK Elevation of Privilege Vulnerability	.NET	Elevation of Privilege
CVE-2026-45491	.NET Tampering Vulnerability	.NET	Tampering
CVE-2026-45497	Microsoft M365 Copilot Remote Code Execution Vulnerability	Microsoft Copilot	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-45500	Microsoft Exchange Server Spoofing Vulnerability	Microsoft Exchange Server	Spoofing
CVE-2026-45501	Microsoft Exchange Server Spoofing Vulnerability	Microsoft Exchange Server	Spoofing
CVE-2026-45502	Microsoft Exchange Server Information Disclosure Vulnerability	Microsoft Exchange Server	Information Disclosure
CVE-2026-45503	Microsoft Exchange Server Information Disclosure Vulnerability	Microsoft Exchange Server	Information Disclosure
CVE-2026-45504	Microsoft Exchange Server Elevation of Privilege Vulnerability	Microsoft Exchange Server	Elevation of Privilege
CVE-2026-45583	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	Remote Code Execution
CVE-2026-45586	Windows Collaborative Translation Framework (CTFMON) Elevation of Privilege Vulnerability	Windows Collaborative Translation Framework	Elevation of Privilege
CVE-2026-45588	Secure Boot Security Feature Bypass Vulnerability	Windows Secure Boot	Security Feature Bypass
CVE-2026-45591	ASP.NET Core Denial of Service Vulnerability	ASP.NET Core	Denial of Service
CVE-2026-45592	Windows Internet (wininet.dll) Elevation of Privilege Vulnerability	Windows Internet (wininet.dll)	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-45593	Windows SDK Elevation of Privilege Vulnerability	Windows SDK	Elevation of Privilege
CVE-2026-45594	Windows Application Identity (AppID) Information Disclosure Vulnerability	Windows Application Identity (AppID) Subsystem	Information Disclosure
CVE-2026-45595	Windows Mark of the Web Security Feature Bypass Vulnerability	Windows Mark of the Web (MOTW)	Security Feature Bypass
CVE-2026-45596	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-45597	Windows UI Automation Manager (uiamanager.dll) Elevation of Privilege Vulnerability	UI Automation Manager (uiamanager.dll)	Elevation of Privilege
CVE-2026-45598	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-45599	Windows UPnP Device Host Remote Code Execution Vulnerability	Universal Plug and Play (upnp.dll)	Remote Code Execution
CVE-2026-45600	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	Windows Kernel-Mode Drivers	Elevation of Privilege
CVE-2026-45601	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-45602	Windows Dynamic Host Configuration Protocol (DHCP) Tampering Vulnerability	Windows DHCP Server	Tampering
CVE-2026-45603	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-45604	Windows Managed Installer Information Disclosure Vulnerability	Windows Application Identity (AppID) Subsystem	Information Disclosure
CVE-2026-45605	Windows Bluetooth Service Elevation of Privilege Vulnerability	Windows Bluetooth Service	Elevation of Privilege
CVE-2026-45606	Microsoft UxTheme Library (uxtheme.dll) Denial of Service Vulnerability	Microsoft UxTheme Library (uxtheme.dll)	Denial of Service
CVE-2026-45607	Windows Hyper-V Remote Code Execution Vulnerability	Windows Hyper-V	Remote Code Execution
CVE-2026-45608	Windows DHCP Client Information Disclosure Vulnerability	Windows DHCP Client	Information Disclosure
CVE-2026-45634	Windows DHCP Client Information Disclosure Vulnerability	Windows DHCP Server	Information Disclosure
CVE-2026-45635	Windows UPnP Device Host Remote Code Execution Vulnerability	Universal Plug and Play (upnp.dll)	Remote Code Execution
CVE-2026-45636	Windows NTFS Remote Code Execution Vulnerability	Windows NTFS	Remote Code Execution
CVE-2026-45637	Microsoft DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege
CVE-2026-45638	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-45639	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability	Windows RDP	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2026-45640	Windows Bluetooth Port Driver Elevation of Privilege Vulnerability	Windows Bluetooth Port Driver	Elevation of Privilege
CVE-2026-45641	Windows Hyper-V Remote Code Execution Vulnerability	Role: Windows Hyper-V	Remote Code Execution
CVE-2026-45642	Microsoft Azure Attestation service and Device Health Attestation Service Spoofing Vulnerability	Microsoft Azure Attestation service and Device Health Attestation Service	Spoofing
CVE-2026-45643	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution
CVE-2026-45644	Microsoft Live Share Canvas SDK Elevation of Privilege Vulnerability	Microsoft Live Share Canvas SDK	Elevation of Privilege
CVE-2026-45645	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-45647	Microsoft Defender for Endpoint for Mac Elevation of Privilege Vulnerability	Microsoft Defender for Endpoint	Elevation of Privilege
CVE-2026-45648	Windows Active Directory Domain Services Remote Code Execution Vulnerability	Active Directory Domain Services	Remote Code Execution
CVE-2026-45649	Office for Android Spoofing Vulnerability	Office for Android	Spoofing
CVE-2026-45650	Microsoft Bing Search Spoofing Vulnerability	Microsoft Bing	Spoofing
CVE-2026-45653	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-45654	Secure Boot Security Feature Bypass Vulnerability	Windows Secure Boot	Security Feature Bypass
CVE-2026-45655	Windows BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass
CVE-2026-45656	UEFI Secure Boot Security Feature Bypass Vulnerability	Windows UEFI	Security Feature Bypass
CVE-2026-45657	Windows Kernel Remote Code Execution Vulnerability	Windows Kernel	Remote Code Execution
CVE-2026-45658	Windows BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass
CVE-2026-47281	Visual Studio Code Elevation of Privilege Vulnerability	Visual Studio Code	Elevation of Privilege
CVE-2026-47284	Visual Studio Code Information Disclosure Vulnerability	Visual Studio Code	Information Disclosure
CVE-2026-47287	Visual Studio Code Tampering Vulnerability	Visual Studio Code	Tampering
CVE-2026-47288	Windows Kerberos Key Distribution Center (KDC) Remote Code Execution	Windows Kerberos	Remote Code Execution
CVE-2026-47289	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2026-47291	HTTP.sys Remote Code Execution Vulnerability	Windows HTTP.sys	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-47292	Visual Studio Code MSSQL Extension Remote Code Execution Vulnerability	Visual Studio Code	Elevation of Privilege
CVE-2026-47293	Microsoft Office Click-To-Run Elevation of Privilege Vulnerability	Microsoft Office Click-To-Run	Elevation of Privilege
CVE-2026-47298	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-47631	Microsoft Exchange Server Spoofing Vulnerability	Microsoft Exchange Server	Spoofing
CVE-2026-47634	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-47635	Microsoft Outlook and Word Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-47636	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-47637	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-47638	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-47639	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-47640	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing

CVE	NAME	PRODUCT	IMPACT
CVE-2026-47641	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-47643	Azure Stack Edge Remote Code Execution Vulnerability	Azure Stack Edge	Remote Code Execution
CVE-2026-47644	Copilot Chat (Microsoft Edge) Information Disclosure Vulnerability	Copilot Chat (Microsoft Edge)	Information Disclosure
CVE-2026-47648	Windows Storage Elevation of Privilege Vulnerability	Windows Storage	Elevation of Privilege
CVE-2026-47652	Windows Hyper-V Remote Code Execution Vulnerability	Windows Hyper-V	Remote Code Execution
CVE-2026-47653	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2026-47654	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2026-47655	Microsoft Graph Information Disclosure Vulnerability	Microsoft Graph	Information Disclosure
CVE-2026-47656	Windows Boot Manager Security Feature Bypass Vulnerability	Windows Boot Manager	Security Feature Bypass
CVE-2026-48560	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-48562	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing

CVE	NAME	PRODUCT	IMPACT
CVE-2026-48563	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2026-48565	Windows Narrator Braille Elevation of Privilege Vulnerability	Windows Narrator Braille	Elevation of Privilege
CVE-2026-48566	Windows DWM Core Library Information Disclosure Vulnerability	Windows DWM Core Library	Information Disclosure
CVE-2026-48567	Azure HorizonDB Elevation of Privilege Vulnerability	Azure HorizonDB	Elevation of Privilege
CVE-2026-48568	Secure Boot Security Feature Bypass Vulnerability	Windows Secure Boot	Security Feature Bypass
CVE-2026-48569	Visual Studio Code Security Feature Bypass Vulnerability	Visual Studio Code	Security Feature Bypass
CVE-2026-48570	Secure Boot Security Feature Bypass Vulnerability	Windows Secure Boot	Security Feature Bypass
CVE-2026-48573	Secure Boot Security Feature Bypass Vulnerability	Windows Secure Boot	Security Feature Bypass
CVE-2026-48574	Windows Media Remote Code Execution Vulnerability	Windows Media	Remote Code Execution
CVE-2026-48575	Secure Boot Security Feature Bypass Vulnerability	Windows Secure Boot	Security Feature Bypass
CVE-2026-48576	Secure Boot Security Feature Bypass Vulnerability	Windows Secure Boot	Security Feature Bypass

CVE	NAME	PRODUCT	IMPACT
CVE-2026-48578	Secure Boot Security Feature Bypass Vulnerability	Windows Secure Boot	Elevation of Privilege
CVE-2026-48579	Microsoft Exchange Online Information Disclosure Vulnerability	Microsoft Exchange Online	Information Disclosure
CVE-2026-48583	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2026-49160	HTTP.sys Denial of Service Vulnerability	HTTP/2	Denial of Service
CVE-2026-49161	Microsoft PC Manager Security Feature Bypass Vulnerability	Microsoft PC Manager	Security Feature Bypass
CVE-2026-50507	Windows BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass
CVE-2026-50508	Windows NTLM Spoofing Vulnerability	Windows NTLM	Spoofing
CVE-2025-10263	ARM Completion of affected memory accesses might not be guaranteed by completion of a TLBI [kernel] Security Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2026-8863	UEFI Secure Boot Security Feature Bypass Vulnerability	Windows UEFI	Security Feature Bypass

References

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

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 Demo of **HivePro**.

REPORT GENERATED ON

June 10, 2026 • 9:00 AM

More at www.hivepro.com