Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft Patch Tuesday August 2026 - Priority Fixes

Date of Publication	Admiralty Code	TA Number
August 12, 2026	A1	TA2026230

Summary

First Seen: August 12, 2026
Affected Platforms: Microsoft Windows, Microsoft SharePoint Server, GitHub Copilot and Visual Studio Code, Windows Ancillary Function Driver, Visual Studio Code, Desktop Window Manager, Windows Win32k, Windows Deployment Services TFTP Server, Windows DWM Core Library, Windows User Profile Service, Windows DHCP Server, Windows Kernel, Windows Remote Access Connection Manager, Windows Kerberos, Windows HTTP.sys, Windows User-Mode Power Service (UMPS), Windows Cloud Files Mini Filter Driver, Microsoft Digest Authentication, Windows Program Compatibility Assistant Service, Windows MIDI Service Module, Windows Installer, Windows Accessibility Infrastructure, Windows Ancillary Function Driver for WinSock, Microsoft High Performance Computing (HPC) Pack, Windows TCP/IP, Microsoft High Performance Computing (HPC) Pack, Microsoft 365 Admin Center, Microsoft QUIC, Azure SQL Database
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-2026-68820	Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10- 11 26H1	✓	✓	✓
CVE-2026-70355	Microsoft SharePoint Server Elevation of Privilege Vulnerability	Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019	✗	✗	✓
CVE-2026-70335	GitHub Copilot and Visual Studio Code Elevation of Privilege Vulnerability	Visual Studio Code	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-70307	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10- 11 26H1	✗	✗	✓
CVE-2026-69278	Visual Studio Code Security Feature Bypass Vulnerability	Visual Studio Code	✗	✗	✓
CVE-2026-66804	Microsoft Windows Cross Device Service Elevation of Privilege Vulnerability	Windows 10 - 11 26H1	✗	✗	✓
CVE-2026-65788	Desktop Window Manager Elevation of Privilege Vulnerability	Windows Server 2025, Windows 11 26H1	✗	✗	✓
CVE-2026-65775	Windows Win32k Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10- 11 26H1	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-65665	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019	✗	✗	✓
CVE-2026-63520	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016	✗	✗	✓
CVE-2026-62893	Windows Deployment Services TFTP Server Remote Code Execution Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10	✗	✗	✓
CVE-2026-62888	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows Server 2022, 2025, Windows 10 - 11 26H1	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-62832	Windows User Profile Service Elevation of Privilege Vulnerability	Windows Server 2022, 2025, Windows 10 - 11 26H1	✗	✗	✓
CVE-2026-62823	Windows DHCP Server Remote Code Execution Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10	✗	✗	✓
CVE-2026-62788	Windows Kernel Elevation of Privilege Vulnerability	Windows Server 2025, Windows 11 26H1	✗	✗	✓
CVE-2026-62783	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	Windows Server 2019, 2022, 2025, Windows 10 - 11 26H1	✗	✗	✓
CVE-2026-62766	Windows Kerberos Elevation of Privilege Vulnerability	Windows Server 2025, Windows 11 26H1	✗	✗	✓
CVE-2026-62741	Windows HTTP.sys Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10 - 11 26H1	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-62737	Windows Kernel Elevation of Privilege Vulnerability	Windows Server 2025, Windows 11 26H1	✗	✗	✓
CVE-2026-62735	Windows HTTP.sys Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10- 11 26H1	✗	✗	✓
CVE-2026-62721	Windows User-Mode Power Service (UMPS) Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10- 11 26H1	✗	✗	✓
CVE-2026-62713	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Server 2019, 2022, 2025, Windows 10 - 11 26H1	✗	✗	✓
CVE-2026-62712	Windows Win32k Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10- 11 26H1	✗	✗	✓
CVE-2026-62698	Microsoft Digest Authentication Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10- 11 26H1	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-62696	Windows Program Compatibility Assistant Service Elevation of Privilege Vulnerability	Windows Server 2016, 2019, 2022, 2025, Windows 10- 11 26H1	✗	✗	✓
CVE-2026-62688	Windows MIDI Service Module Elevation of Privileges Vulnerability	Windows 11 24H2 - 11 26H1	✗	✗	✓
CVE-2026-61930	Windows Kernel Elevation of Privilege Vulnerability	Windows Server 2016, 2019, 2022, 2025, Windows 10- 11 26H1	✗	✗	✓
CVE-2026-61929	Windows Kernel Elevation of Privilege Vulnerability	Windows Server 2025, Windows 11 23H2 - 11 26H1	✗	✗	✓
CVE-2026-61925	Windows Installer Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10 - 11 26H1	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-61358	Windows Accessibility Infrastructure (ATBroker.exe) Elevation of Privilege Vulnerability	Windows Server 2019, 2022, 2025, Windows 10 - 11 26H1	✗	✗	✓
CVE-2026-61348	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10 - 11 26H1	✗	✗	✓
CVE-2026-59133	Microsoft High Performance Computing (HPC) Pack Elevation of Privilege Vulnerability	Windows App Client for Windows Desktop	✗	✗	✓
CVE-2026-59132	Windows TCP/IP Denial of Service Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10 - 11 26H1	✗	✗	✓
CVE-2026-59124	Microsoft High Performance Computing (HPC) Pack Remote Code Execution Vulnerability	Windows App Client for Windows Desktop	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-58650	Visual Studio Code Security Feature Bypass Vulnerability	Visual Studio Code	✗	✗	✓
CVE-2026-62873	Microsoft 365 Admin Center Elevation of Privilege Vulnerability	Microsoft 365 Admin Center	✗	✗	✓
CVE-2026-62815	Microsoft QUIC Remote Code Execution Vulnerability	Windows Server 2022, 2025, Windows 11 23H2 - 11 26H1	✗	✗	✓
CVE-2026-56162	Azure SQL Database Elevation of Privilege Vulnerability	Azure SQL Database	✗	✗	✓
CVE-2026-72971	Windows Container Isolation FS Filter Driver (unionfs.sys) Tampering Vulnerability	Windows 11 26H1	✗	✗	✓

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

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
Reconnaissance	T1589: Gather Victim Identity Information	
Initial Access	T1190: Exploit Public-Facing Application	
	T1566: Phishing	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1548: Abuse Elevation Control Mechanism	
	T1574: Hijack Execution Flow	
	T1134: Access Token Manipulation	
Defense Evasion	T1211: Exploitation for Defense Evasion	
Execution	T1059: Command and Scripting Interpreter	
	T1204: User Execution	T1204.001: Malicious Link
	T1203: Exploitation for Client Execution	
Impact	T1499: Endpoint Denial of Service	
Credential Access	T1212: Exploitation for Credential Access	
Command and Control	T1071: Application Layer Protocol	

Vulnerability Details

#1

Microsoft's August 2026 Patch Tuesday delivers an extensive batch of security updates, addressing 421 vulnerabilities across its product ecosystem. These include 62 rated critical, 358 marked important, and one moderate in severity. The vulnerabilities span various categories: 111 involve Remote Code Execution (RCE), 177 Elevation of Privilege, 85 Information Disclosure, 12 Denial of Service, 11 Security Feature Bypass, 21 Spoofing, and 4 Tampering issues. Beyond its own products, Microsoft also released patches for 2 non-Microsoft CVEs, pushing the total count of vulnerabilities addressed this month to 423. Notably, 39 of these CVEs are considered at risk of active exploitation, underscoring the urgency of prompt patch deployment.

#2

The most urgent fix this month is for the actively exploited zero-day, CVE-2026-68820, a use-after-free bug in the Windows Ancillary Function Driver for WinSock that lets an already-logged-in attacker gain higher privileges on a device. The flaw is being exploited in the wild, and the Lazarus group has been using it as part of Operation Dream Job, with its latest campaign targeting defense organizations in Europe and India.

#3

Two publicly known flaws round out the list of already-disclosed issues. CVE-2026-62832 affects the Windows User Profile Service, where a link-following flaw allows privilege escalation, while CVE-2026-72971 hits the Container Isolation FS Filter Driver (unionfs.sys), letting an attacker tamper with the system through the same kind of link-resolution weakness.

#4

Microsoft Office SharePoint sees three notable bugs this cycle. A cross-site scripting issue (CVE-2026-70355) can be used to escalate privileges over a network, a deserialization flaw (CVE-2026-65665) opens the door to remote code execution, and a separate input-validation weakness (CVE-2026-63520) also allows remote code execution without needing prior access.

#5

Developer tools weren't spared either. GitHub Copilot and Visual Studio Code carry an OS command injection bug (CVE-2026-70335) that lets a local attacker escalate privileges, along with two authorization-related flaws in VS Code (CVE-2026-69278 and CVE-2026-58650) that allow attackers to slip past security protections locally.

#6

A large chunk of this month's fixes are privilege-escalation bugs buried deep in Windows components, mostly use-after-free and heap overflow issues that require local access. These include repeated flaws in the WinSock driver (CVE-2026-70307, CVE-2026-61348), Windows Kernel (CVE-2026-62788, CVE-2026-61930, CVE-2026-61929, CVE-2026-62737), Win32K (CVE-2026-65775, CVE-2026-62712), the Desktop Window Manager and DWM Core Library (CVE-2026-65788, CVE-2026-62888), and HTTP.sys (CVE-2026-62741, CVE-2026-62735). Similar issues also turn up in the Cross Device Service, Kerberos, Remote Access Connection Manager, the Cloud Files Mini Filter Driver, Digest Authentication, the Program Compatibility Assistant Service, the MIDI Service Module, Windows Installer, and the Accessibility Infrastructure component (ATBroker.exe).

#7

On the network-facing side, a handful of bugs stand out for allowing remote code execution without any local access needed. Windows Deployment Services has a use-after-free flaw (CVE-2026-62893), the Windows DHCP Server carries a heap overflow reachable from an adjacent network (CVE-2026-62823), Microsoft's HPC Pack has a deserialization bug (CVE-2026-59124), and Microsoft QUIC includes a use-after-free issue (CVE-2026-62815) that could also lead to code execution.

#8

Finally, a few cloud and service-level issues round out the update: HPC Pack also has a privilege escalation flaw tied to unnecessary permissions (CVE-2026-59133), Windows TCP/IP has a null pointer bug that can crash a system remotely (CVE-2026-59132), Microsoft 365 Admin Center has a signature verification flaw allowing privilege escalation (CVE-2026-62873), and Azure SQL Database has an authentication weakness that could let an attacker gain elevated access over the network (CVE-2026-56162).

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 vulnerability and publicly disclosed vulnerabilities CVE-2026-68820, CVE-2026-62832, and CVE-2026-72971. 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.

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2b4987c07a3d9a9a5d1a9bf4efa3d1903e775090b611710edafdc92874265ca8, 3a02d0d798e8d35555776886d92b20ff38a101c9ef7e0eebc8ce5d259516525a, 92106b0c62a0a42678232f8273f030b2d3c8e92efce81b98b9eec70cfe98afa1, 396192d92d17ace1a521f1351eeeba2825e60badd0d799cc5c338e4934b3c82c, f7e620134ca935067797ab957317b346ce0df84a4e9b9ca54a6acc9b75afda4d, 75b93a7103b0562f6497d30052c0c5cf7aa58c1bf0e9297022b74469a7f096f1, a45144d22cac70a45d71cf4dffa4efbc373658779a56cf1300d6ac863d6cc7e2, 1de949c71efcfb0ffc41f33d38833dbc4b082075b1a540fc68c18c535d7ad86c, 4c9b804d6155b29f1e27a9ffe531e10bc42a7bdab42f905b50146bf2026768d9, 29e24c007549e51319ff3aee011da6f9f93568e8c85a5ad69c9e53bd3f4533a2, 4ebdce2f47c23ff8c9e8e80c8b5239c7a5764da31cd3ab8f0505926890adc105, c2aa28bb5e2a749c693712008276f311edd912f689371ef9e8a1ee5fb4167461, 2db25ac41a66aa523c79e23e00443573530dd7bd82b8371bcc87bd7232e141eb, 5278ee922838352f1480a73e971161017d643a80b7ec22bf725897dfd088696d, b4082d21070d9ddf53fde4ea22524d09e41ec9826ce63cef3c6235e458d21afb, fb3fc5626f68677fb1269a2fefbe70e719211b4065e836ab92e06a8210139a2d, ea7056f2bf36c66a61ff787ff5be975a85f534c3c5ca178791dac2504db2c619, 13d10bc99f7f7abe7ee0902be87920b73b2ea41bd9683dbfcad340dacbcdef79, 4fd32432341dfcf54d0517a6bbc38e5d265be70933493e4183c2a340cdde9a2d, 4dd792c9f672bbdcc8d363d745994efe90f4ffc5fdc2c059c8e379a48ad6a68a, ba96c603e44046de703c67b2c3b7e4ca974afef7b437a0244418bc4edc781bb7,

TYPE	VALUE
SHA256	72dccae85e062f541fecad9ec7a18a3123e7ae5ac5d53c91709b53a46dbbd289, 231b1ef8b95bf77887d5377e2a60f649035e78f543af1b82877db36a5759d858, 6da9b1e6f3315ceb77dd14a937a26cc3602bf6a7e2c2ecafb3c65ce5319837be, a0578a2b7821d7e2c573530648f26d7a0d98b373ab24fb7f0c792736761e542d, 82268052f94df6f4870d02e57b18d4c54136cc7a8c8d80ad162631f99462c943, 3b6378df8442e63a6ed7317075913e4720847a510d95022d4a8347b2637c245d, a673ae661593c0de9bbb815593b816a6853dad6d55ad5042d2ef1875cd13d6e7, 8ce6c29f92dc45b1474417cbdff4ed0c18e58fa63e3a071ee9f85aa9d2aac07c, acb97cec84e08b89f41967a24e965d1fd2c51751cef158f7aa35bb4306b87b97, 3601060c62edeeaa49def6a13be6e126e1024ce011faad4e2d9f585ccf6bd5a6, fecf12088843801215898442bd1ff3e266f29d14e29a94780e857f69c4915d6b, d578c28c9afe7457a0d81f6701332ef8197e8f7468de654935fb29a50ea66459, 743172aab606974b054a64561534ae66baa3a840657f79d7c6fa18350e8d45d1, db3d69b7eeda2e35e23006bf4b7e206281fce809584207214fc213f9bc30376d, 590fb6ae19480d694e08ee85859cad8066f2f87e7e5abba2960c6d115e1615d6, 68d4fba7b1300a59cd6212c08910a260cd71b40cd9f51cac933030a68faac0bb, a738059ce07c951c31ab2da3d93d8f69bff32f9b7d933dbf5943441b9cc99075, 21c3ad4838c4324bc5f081021da5fb2e9073d0c9304087811c21eb47c9e22762, cc4e06aa378a190f71384c03023bb3d18a6d66e297d46701220e132963d2e222
Domains	envell[.]xyz, enveil[.]online, uxtramine[.]org
IPv4	135[.]181[.]67[.]203, 135[.]181[.]185[.]158

References

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

https://msrc.microsoft.com/update-guide/vulnerability

https://research.checkpoint.com/2026/shattering-the-dream-when-a-job-offer-becomes-a-zero-day-attack/

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

August 12, 2026 • 08:00 AM

More at www.hivepro.com