Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft Patch Tuesday July 2026 - Priority Fixes

Date of Publication	Admiralty Code	TA Number
July 15, 2026	A1	TA2026199

Summary

First Seen: July 14, 2026
Affected Platforms: Microsoft SharePoint, Windows Server, DHCP Server, Microsoft Active Directory, Microsoft Dynamics NAV and Microsoft Dynamics 365 Business Central, Minecraft Bedrock, Microsoft Office, Microsoft Exchange, Windows BitLocker, Windows DHCP Server
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-2026-56164	Microsoft SharePoint Server Missing Authentication for Critical Function Vulnerability	Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016	✓	✓	✓
CVE-2026-56155	Microsoft Active Directory Federation Services Insufficient Granularity of Access Control Vulnerability	Windows 10, Windows Server 2012, 2016, 2019, 2022, 2025	✓	✓	✓
CVE-2026-58644	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016	✗	✗	✓
CVE-2026-56188	Windows Server Network driver Remote Code Execution Vulnerability	Windows 10 - 11 25H2, Windows Server 2012, 2016, 2019, 2022, 2025	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-56159	DHCP Server Service Remote Code Execution Vulnerability	Windows 10, Windows Server 2012, 2016, 2019, 2022, 2025	✗	✗	✓
CVE-2026-55944	Microsoft Dynamics NAV and Microsoft Dynamics 365 Business Central (On Premises) Remote Code Execution Vulnerability	Microsoft Dynamics NAV 2018	✗	✗	✓
CVE-2026-55047	Microsoft Office Information Disclosure Vulnerability	Microsoft Office 2019, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft Office 365 for Mac, Microsoft Office 2016, Microsoft Office LTSC for Mac 2024, Microsoft Office LTSC 2024, Microsoft SharePoint Server Subscription Edition, Microsoft Office LTSC 2021, Microsoft Office LTSC for Mac 2021, Microsoft 365 Apps for Enterprise	✗	✗	✓
CVE-2026-55040	Microsoft SharePoint Server Security Feature Bypass Vulnerability	Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016	✗	✗	✓
CVE-2026-55010	Minecraft Bedrock Dedicated Server Remote Code Execution Vulnerability	Minecraft Bedrock Dedicated Server	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-54998	Microsoft Exchange Online Elevation of Privilege Vulnerability	Microsoft Exchange Online	✗	✗	✓
CVE-2026-50661	Windows BitLocker Security Feature Bypass Vulnerability	Windows 10 - 11 26H1, Windows Server 2016, 2019, 2022, 2025	✗	✗	✓
CVE-2026-50522	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016	✗	✗	✓
CVE-2026-50518	Windows DHCP Server Remote Code Execution Vulnerability	Windows 10, Windows Server 2012, 2016, 2019, 2022, 2025	✗	✗	✓
CVE-2026-13774	Chromium Use after free in Extensions Vulnerability	Google Chromium	✗	✗	✓
CVE-2026-14382	Chromium Insufficient validation of untrusted input in ANGLE Vulnerability	Google Chromium	✗	✗	✓

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	
Execution	T1203: Exploitation for Client Execution	
	T1059: Command and Scripting Interpreter	
Persistence	T1176: Software Extensions	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	
Defense Evasion	T1211: Exploitation for Defense Evasion	
Credential Access	T1556: Modify Authentication Process	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Vulnerability Details

#1

Microsoft's July 2026 Patch Tuesday stands out as one of the largest security releases the company has ever shipped, addressing the highest number of flaws to date with fixes for 622 vulnerabilities across its product ecosystem. Of these, 63 are rated Critical, 552 Important, 6 Moderate, and 1 Low. The patched flaws cover a wide spread of vulnerability types, including 164 remote code execution issues, 256 elevation of privilege flaws, 109 information disclosure bugs, 35 denial-of-service vulnerabilities, 29 spoofing issues, 21 security feature bypasses, and 8 tampering weaknesses. Beyond its own products, Microsoft also rolled out patches for 428 non-Microsoft CVEs, pushing the total number of vulnerabilities resolved this month to 1,050. We've flagged 15 CVEs from this release as being at risk of active exploitation. These represent the top patching priorities this cycle, and organizations should remediate them before working through the remaining fixes.

#2

Two zero-day vulnerabilities were fixed this month. CVE-2026-56164 is a missing-authentication flaw in Microsoft Office SharePoint that lets an unauthenticated attacker elevate privileges over a network. CVE-2026-56155 stems from insufficiently granular access control in Active Directory Federation Services (AD FS) and allows an authenticated attacker to elevate privileges locally. One flaw was publicly disclosed ahead of patching: CVE-2026-50661 in Windows BitLocker. Caused by a protection mechanism failure, it allows an attacker with physical access to bypass a security feature.

#3

Several critical SharePoint flaws also feature prominently this cycle. CVE-2026-58644 involves deserialization of untrusted data and enables remote code execution over a network. CVE-2026-55040 is a weak-authentication issue that lets an unauthenticated attacker bypass a security feature remotely. CVE-2026-50522 similarly allows an unauthenticated attacker to run code over a network.

#4

The release also tackles a number of high-impact flaws across other Windows components and services. CVE-2026-56188 in the Windows Server network driver permits remote code execution. CVE-2026-56159 and CVE-2026-50518 are both heap-based buffer overflows in the Windows DHCP Server, each allowing remote code execution. CVE-2026-55944 is a deserialization flaw in Microsoft Dynamics NAV that enables code execution over a network, and CVE-2026-55010 is a heap-based buffer overflow in the Minecraft Bedrock Dedicated Server with the same effect. Rounding out the set, CVE-2026-54998 in Microsoft Exchange Online lets an authenticated attacker elevate privileges over a network.

#5

On the non-Microsoft side, two Google Chrome flaws stand out. CVE-2026-13774 is a high-severity issue in versions prior to 150.0.7871.47, where a user tricked into installing a malicious extension could have arbitrary code executed via a crafted Chrome extension. CVE-2026-14382 affects ANGLE in Chrome versions before 150.0.7871.46 and could let a remote attacker attempt a sandbox escape through a crafted HTML page. Taken together, Microsoft's July 2026 updates reflect just how complex and fast-moving today's threat landscape has become. With multiple zero-days, privilege escalation flaws, and remote code execution vulnerabilities all addressed in a single release, organizations are strongly urged to apply these patches without delay, reducing their exposure to 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-2026-56164, CVE-2026-56155, and CVE-2026-50661. 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.

References

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

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

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

July 15, 2026 • 08:30 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com