TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

July 14, 2026

Executive Summary

The Microsoft Security Response Center (MSRC) reported a record-breaking 570 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 570 total patched bugs, fifty-eight (58) were classified as critical severity. Two (2) actively exploited zero-day vulnerabilities (CVE-2026-56155, CVE-2026-56164) and one (1) publicly disclosed zero-day vulnerability (CVE-2026-50661) were included in this Patch Tuesday release. The number of vulnerabilities in each category is listed below:

- 249 Elevation of Privilege
- 143 Remote Code Execution (RCE)
- 102 Information Disclosure
- 17 Security Feature Bypass
- 35 Denial of Service (DoS)
- 16 Spoofing
- 8 Tampering

Featured Critical Vulnerabilities

The 58 critical vulnerabilities listed in July's Patch Tuesday security update are listed below.

Active Directory Certificate Services	Active Directory Domain Services	Microsoft Copilot	Microsoft Dynamics NAV	Microsoft Exchange Server	Minecraft Bedrock Dedicated Server
CVE-2026-54121	CVE-2026-49164	CVE-2026-48561	CVE-2026-55944	CVE-2026-55008	CVE-2026-55010
Remote Desktop Client	**Windows DHCP Client**	**Windows Message Queuing Queue Manager**	**Windows Print Spooler Components**	**Windows Secure Socket Tunneling Protocol**	**Windows TCP/IP**
CVE-2026-50474	CVE-2026-54128	CVE-2026-54992	CVE-2026-58608	CVE-2026-50694	CVE-2026-54999
Reliable Multicast Transport Driver	**Windows GDI+**	**Windows Hyper-V**	**Windows Secure Kernel Mode**	**Microsoft Office Powerpoint**	**Microsoft Office Sharepoint**
CVE-2026-54982 CVE-2026-54995	CVE-2026-49796 CVE-2026-50380	CVE-2026-50680 CVE-2026-54127	CVE-2026-42982 CVE-2026-50392	CVE-2026-55043 CVE-2026-55120 CVE-2026-55123	CVE-2026-50522 CVE-2026-55040 CVE-2026-58644
Windows Server Update Service	**Windows Server Network Driver**	**Windows Media**	**Microsoft Defender**	**Windows DirectX**	**Windows VMSwitch**
CVE-2026-50444	CVE-2026-56188	CVE-2026-50327 CVE-2026-50655 CVE-2026-58542	CVE-2026-55011 CVE-2026-55012	CVE-2026-50382	CVE-2026-57092
Microsoft Office Word	**Windows DHCP Server**	**Microsoft Windows Media Foundation**	**Windows DirectX**	**Microsoft Office**	**Microsoft Office (cont.)**
CVE-2026-55033 CVE-2026-55127 CVE-2026-55132	CVE-2026-48564 CVE-2026-50370 CVE-2026-50518 CVE-2026-56159	CVE-2026-56189 CVE-2026-57087 CVE-2026-57090 CVE-2026-57094	CVE-2026-50382	CVE-2026-50301 CVE-2026-50314 CVE-2026-50467 CVE-2026-55018 CVE-2026-55022	CVE-2026-55045 CVE-2026-55049 CVE-2026-55056 CVE-2026-55129 CVE-2026-55140

TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

July 14, 2026

Safeguards/Recommendations

Organizations should back up all systems, software, data, and device settings prior to performing updates and security patches. Users can regularly monitor the “Check for Updates” window in their Windows device settings to check if systems are up-to-date with the latest security patches.

For a full list of affected products, features, and roles, visit MSRC’s July’s 2026 Patch Tuesday release notes.

References

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