TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

August 11, 2026

Executive Summary

The Microsoft Security Response Center (MSRC) reported 398 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 398 total patched bugs, fourty-two (42) were classified as critical severity. Two (2) publicly disclosed zero-day vulnerabilities (CVE-2026-62832, CVE-2026-72971) and one (1) actively exploited zero-day vulnerability (CVE-2026-68820) were included in this Patch Tuesday release. The number of vulnerabilities in each category is listed below:

- 162 Elevation of Privilege
- 108 Remote Code Execution (RCE)
- 84 Information Disclosure
- 11 Security Feature Bypass
- 12 Denial of Service (DoS)
- 17 Spoofing
- 4 Tampering

Featured Critical Vulnerabilities

The 42 critical vulnerabilities listed in August's Patch Tuesday security update are listed below.

Active Directory Certificate Services	Microsoft Azure Attestation service and Device	Microsoft Exchange Server	Windows Key Guard	Windows iSCSI
CVE-2026-62818	CVE-2026-71331 CVE-2026-66802	CVE-2026-62911	CVE-2026-66799	CVE-2026-65791
Remote Desktop Client	**Windows Deployment Services**	**Windows DHCP Server**	**Windows Routing and Remote Access Services (RRAS)**	**Microsoft QUIC**
CVE-2026-62824	CVE-2026-62893	CVE-2026-62823	CVE-2026-62819	CVE-2026-62815
Reliable Multicast Transport Driver	**Windows Secure Socket Tunneling Protocol**	**Windows GDI+**	**Windows DNS**	**Microsoft Office Excel**
CVE-2026-62816	CVE-2026-62889	CVE-2026-62890 CVE-2026-62822	CVE-2026-65789 CVE-2026-62878 CVE-2026-62820 CVE-2026-62817	CVE-2026-68816 CVE-2026-68804 CVE-2026-68794
Microsoft Office SharePoint	**Microsoft Office Word**	**Microsoft Office**	**Microsoft Office (cont.)**	**Microsoft Office (cont.)**
CVE-2026-65665 CVE-2026-64921 CVE-2026-62827	CVE-2026-64907 CVE-2026-63525 CVE-2026-63518	CVE-2026-70130 CVE-2026-66807 CVE-2026-65664 CVE-2026-65657 CVE-2026-64911	CVE-2026-64910 CVE-2026-64909 CVE-2026-64903 CVE-2026-64898 CVE-2026-63532	CVE-2026-63526 CVE-2026-63519 CVE-2026-63515 CVE-2026-63513

TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

August 11, 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 August’s 2026 Patch Tuesday release notes.

References

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