TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

September 08, 2026

Executive Summary

The Microsoft Security Response Center (MSRC) reported a record-breaking 966 vulnerabilities across Windows, Microsoft Office, SQL Server, Azure services, and other Microsoft products and components. According to the MSRC security update data, 105 vulnerabilities were classified as Critical severity. Additionally, Microsoft addressed two actively exploited zero-day vulnerabilities: CVE-2026-81963 (Windows Update Stack EoP) and CVE-2026-85880 (Windows ALPC EoP).

- 438 Elevation of Privilege
- 258 Remote Code Execution (RCE)
- 173 Information Disclosure
- 19 Security Feature Bypass
- 56 Denial of Service (DoS)
- 16 Spoofing

Featured Critical Vulnerabilities

The 105 critical vulnerabilities listed in September's Patch Tuesday security update are listed below.

Windows Hello	**Windows Secure Kernel Mode**	**Microsoft Office Excel**	**Microsoft Office Outlook**	**Microsoft Office**	**Microsoft Graphics Component**
CVE-2026-81354, CVE-2026-69799, CVE-2026-69784, CVE-2026-69864, CVE-2026-69725, CVE-2026-69710, CVE-2026-69820, CVE-2026-69740, CVE-2026-72980	CVE-2026-83939, CVE-2026-69906, CVE-2026-69846, CVE-2026-69501	CVE-2026-81948, CVE-2026-81949, CVE-2026-81950, CVE-2026-81951, CVE-2026-81953, CVE-2026-81959	CVE-2026-78525, CVE-2026-78520, CVE-2026-78519, CVE-2026-78509	CVE-2026-69632, CVE-2026-77898, CVE-2026-69285, CVE-2026-78505	CVE-2026-81955, CVE-2026-73006, CVE-2026-78439, CVE-2026-77493
SQL Server	**Windows DNS**	**Windows Imaging Component**	**Routing and Remote Access Service (RRAS)**	**Reliable Multicast Transport Driver (RMCAST)**	**Windows Services for NFS ONCRPC XDR Driver**
CVE-2026-65669, CVE-2026-67643, CVE-2026-67636, CVE-2026-67378, CVE-2026-67631	CVE-2026-72987, CVE-2026-69813, CVE-2026-69858, CVE-2026-69730, CVE-2026-65789, CVE-2026-62878, CVE-2026-62820, CVE-2026-62817	CVE-2026-73023, CVE-2026-73013, CVE-2026-69499, CVE-2026-70296, CVE-2026-77495, CVE-2026-69860	CVE-2026-69590, CVE-2026-72959, CVE-2026-72950, CVE-2026-69852	CVE-2026-69530, CVE-2026-78449, CVE-2026-78450	CVE-2026-69595, CVE-2026-78445, CVE-2026-70585
Windows Deployment Services	**Microsoft Office PowerPoint**	Microsoft Office Word	**Windows Hyper-V**	**Microsoft Windows Codecs Library**	**Windows Media Player**
CVE-2026-72954, CVE-2026-72957, CVE-2026-62893	CVE-2026-69797, CVE-2026-69767, CVE-2026-69678	CVE-2026-81952, CVE-2026-77504, CVE-2026-78510	CVE-2026-72961, CVE-2026-80083, CVE-2026-69603	CVE-2026-81352, CVE-2026-58599	CVE-2026-70203, CVE-2026-72960
Graphic Fonts	**Windows Failover Cluster**	**Windows DHCP Server**	**Windows Virtualization-Based Security (VBS) Enclave**	**Windows Credential Guard**	**Windows ALPC**
CVE-2026-73018, CVE-2026-72986	CVE-2026-73010, CVE-2026-78444	CVE-2026-69845, CVE-2026-72979, CVE-2026-62823	CVE-2026-83498, CVE-2026-83501	CVE-2026-72958	CVE-2026-69874

TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

September 08, 2026

Windows Virtual Trusted Platform Module CVE-2026-69890	**Windows USB Video Driver** CVE-2026-72962	**Windows Graphics Kernel** CVE-2026-73017	**Windows HTTP Print Provider** CVE-2026-69769	**Windows Shell** CVE-2026-69829	**Windows Netlogon** CVE-2026-72982
Role DNS Server CVE-2026-77505, CVE-2026-69827	**Windows Kerberos** CVE-2026-69676	**Windows Key Distribution Center** CVE-2026-69712	**Windows Secure Socket Tunneling Protocol (SSTP)** CVE-2026-73009	**Windows Message Queuing** CVE-2026-69579	**Windows Remote Desktop** CVE-2026-69518
Windows Raw Image Extension CVE-2026-69649	**Windows Paint** CVE-2026-70586	**Windows Internet Connection Sharing (ICS)** CVE-2026-72983	**IP Helper** CVE-2026-72983	**Virtual Hard Disk (VHD) Miniport Driver** CVE-2026-81355	**Microsoft Windows Media Foundation** CVE-2026-69601
Microsoft WebP Image Extension CVE-2026-70351	**Skype for Business** CVE-2026-66302	**Microsoft Dynamics 365 On-Premises** CVE-2026-65772			

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 September’s 2026 Patch Tuesday release notes.

References

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