

Microsoft Patch Tuesday

November 10, 2026

Executive Summary

The Microsoft Security Response Center (MSRC) reported 1,094 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 1,094 total patched bugs, sixty-four (64) were classified as critical severity. One (1) actively exploited zero-day vulnerability (CVE-2026-124194) was included in this Patch Tuesday release. The number of vulnerabilities in each category is listed below:

- 535 Elevation of Privilege
- 296 Remote Code Execution (RCE)
- 156 Information Disclosure
- 28 Security Feature Bypass
- 46 Denial of Service (DoS)
- 22 Spoofing
- 11 Tampering

Featured Critical Vulnerabilities

The 64 critical vulnerabilities listed in November's Patch Tuesday security update are listed below.

Microsoft Office Excel	Microsoft Office Excel (cont.)	Windows Hyper-V	Microsoft Office Word	Microsoft Office Outlook	Windows Message Queuing
CVE-2026-124170	CVE-2026-118711	CVE-2026-119960	CVE-2026-124185	CVE-2026-111309	CVE-2026-119964
CVE-2026-120789	CVE-2026-118702	CVE-2026-119947	CVE-2026-111285	CVE-2026-110068	CVE-2026-119963
CVE-2026-120788	CVE-2026-118701	CVE-2026-113865	CVE-2026-110067	CVE-2026-110043	CVE-2026-116710
CVE-2026-120786	CVE-2026-118297	CVE-2026-113864	CVE-2026-110047		
CVE-2026-118730	CVE-2026-118296	CVE-2026-113861			
CVE-2026-118713	CVE-2026-118292	CVE-2026-113860			
Active Directory Domain Services	**Microsoft Office**	**Windows Graphics Kernel**	**Windows Hyper-V (cont.)**	**Windows Message Queuing Queue Manager**	**Azure Managed Grafana**
CVE-2026-118148	CVE-2026-120003	CVE-2026-125137	CVE-2026-113856	CVE-2026-119967	CVE-2026-114160
CVE-2026-118146	CVE-2026-111289	CVE-2026-119966	CVE-2026-113753	CVE-2026-109459	
Azure OpenAI	**Entra Device Registration**	**Graphic Fonts**	**Microsoft Defender**	**Microsoft Exchange Server**	**Microsoft Office PowerPoint**
CVE-2026-119990	CVE-2026-109469	CVE-2026-119969	CVE-2026-122194	CVE-2026-118207	CVE-2026-120005

Copyright © 2026. Security Risk Advisors Intl, LLC. All Rights Reserved *Version 1. Initial Report*



Microsoft Patch Tuesday

November 10, 2026

Microsoft Windows Codecs Library CVE-2026-113749	**Microsoft Windows Search Component** CVE-2026-116928	**Windows Cred SSProvider Protocol** CVE-2026-119962	**Windows Deployment Services** CVE-2026-119951	**Windows Function Discovery Resource Publication** CVE-2026-125134	**Windows Function Discovery SSDP Provider** CVE-2026-118145
Windows Internet Information Services CVE-2026-119961	**Windows LDAP - Lightweight Directory Access Protocol** CVE-2026-119958	**Windows Network Address Translation (NAT)** CVE-2026-113862	**Windows Network Connected Devices Auto-Setup Service** CVE-2026-125136	**Windows Print Spooler Components** CVE-2026-113752	**Windows Raw Image Extension** CVE-2026-114169
Windows Remote Desktop Services CVE-2026-119957	**Windows Remote Procedure Call Runtime** CVE-2026-118737	**Windows SMB Server Network Transport Driver (srvnet.sys)** CVE-2026-113825	**Windows Schannel** CVE-2026-119952	**Windows TCP/IP** CVE-2026-113859	**Windows TPM** CVE-2026-119382
Windows Xbox Live Networking Service CVE-2026-112967					

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 November's 2026 Patch Tuesday release notes.

References

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

Copyright © 2026. Security Risk Advisors Intl, LLC. All Rights Reserved *Version 1. Initial Report*