

# Patch Tuesday

ivanti

NOV 2024

Microsoft



7

Bulletins

2









Critical

4

Important

The top priority for the November 2024 Patch Tuesday is the Windows OS update to resolve two known exploited CVEs (CVE-2024-49039 and CVE-2024-43451).

For organizations running Microsoft Exchange Server you will also want to prioritize this month's Exchange Server update which resolves a Publicly Disclosed vulnerability (CVE-2024-49040) which included proof-of-concept exploit code making it a much more likely risk that threat actors will take advantage and target this vulnerability.

	Affected products	CVE count	Impact	Vendor severity	Ivanti priority	Threat risk	Exploits	Disclosures
MS24-11-EXCH	Microsoft Exchange Server 2016 and 2019	1	Spoofing	Important	1			CVE-2024-49040
MS24-11-O365	Microsoft 365 Apps, Office 2019, Office LTSC 2021, and Office LTSC 2024	8	Remote Code Execution	Important	2			
MS24-11-OFF	Excel 2016, Office 2016, Office 2021 & 2024 LTSC for Mac, Office Online Server, and Word 2016	8	Remote Code Execution	Important	2			
MS24-11-SPT	Sharepoint Server 2016 - 2019	0	None Reported	Unrated	3			
MS24-11-SQL	SQL Server 2016 - 2022	31	Remote Code Execution	Important	2			
MS24-11-W10	Windows 10, Server 2016, Server 2019, Server 2022, Edge Chromium and IE 11	36	Remote Code Execution	Critical	1		CVE-2024-43451, CVE-2024-49039	CVE-2024-49019
MS24-11-W11	Windows 11, Server 2025, and Edge Chromium	35	Remote Code Execution	Critical	1		CVE-2024-43451, CVE-2024-49039	CVE-2024-49019