



Easing into 2024 with a light release from Microsoft and third-party updates from Google and Mozilla; expect a quarterly update from Oracle next week to complete your lineup this month. Microsoft has resolved 49 new CVEs and 7 CVEs from 2023 to expand the affected products to include additional updates. No Public Disclosures or Exploited reports at this time so business as usual. The two critical CVEs in the OS update this month are the highest risk. Get things evaluated and tested as part of your normal maintenance schedule.

For more information visit: ivanti.com/patch-tuesday

Microsoft Bulletins	Affected products	CVE count	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
MS24-01-MRNET	.NET Framework 2.0 SP2 - 4.8.1	3	Security Feature Bypass	Important	2	■■■■	
MS24-01-O365	Microsoft 365 Apps, Office 2019, and Office LTSC 2021	1	Remote Code Execution	Important	2	■■■■	
MS24-01-SONET	.NET Framework 2.0 SP2 - 4.8.1	3	Security Feature Bypass	Important	2	■■■■	
MS24-01-SPT	Sharepoint Server 2016- 2019	1	Remote Code Execution	Important	2	■■■■	
MS24-01-SQL	SQL Server 2022	1	Security Feature Bypass	Important	2	■■■■	
MS24-01-W10	Windows 10, Server 2016, Server 2019, Server 2022, Edge Chromium and IE 11	39	Remote Code Execution	Critical	1	■■■●	
MS24-01-W11	Windows 11 and Edge Chromium	35	Remote Code Execution	Critical	1	■■■●	
Google Bulletin	Affected products	CVE count	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
CHROME-240109	Google Chrome	1	Security Feature Bypass	High	1	■■■●	