ivanti Patch Tuesday

October 10, 2023

Microsoft

11	6	5
Bulletins	Critical	Important

It has been a long road to October Patch Tuesday and many of you may be experiencing Zero-day fatigue. Apple had five zero-day vulnerabilities across most of their products culminating in their updates that released on September 26th (which also included the EoL of Big Sur). Google and Mozilla continued to be busy with several zero-day vulnerabilities in open-source library, Libwebp. This also impacted chromium-based browsers like Microsoft Edge, Opera and others. For more details on the lineup of CVEs leading up to October Patch Tuesday check out our Patch Tuesday Forecast on HelpNetSecurity.

Microsoft has resolved 104 new CVEs this month, three of which are flagged as exploited. The lineup from Microsoft includes Windows, Office 365, SQL Server, Exchange Server, and multiple Azure components. Along with the large lineup of fixes October also marks the end-of-life for Windows Server 2012 and 2012 R2.

Microsoft Bulletins	Affected products	CVE count	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
MS23-10-EXCH	Microsoft Exchange Server 2016 - 2019	1	Remote Code Execution	Important	2	■■□□	
MS23-10-IE	Internet Explorer 11	1	Remote Code Execution	Important	2	■■□□	
MS23-10-MR8	Server 2012 and IE	60	Remote Code Execution	Critical	1	■■■■	Known Exploited and Publicly Disclosed: CVE-2023-36563
MS23-10-MR81	Server 2012 R2 and IE	61	Remote Code Execution	Critical	1	■■■■	Known Exploited and Publicly Disclosed: CVE-2023-36563
MS23-10-OFF	Office for Andriod, Office for Universal, Office 2019 & LTSC 2021 for Mac, and Skype for Business Server 2015 & 2019	5	Remote Code Execution	Important	1	■■■■	Known Exploited and Publicly Disclosed: CVE-2023-41763
MS23-10-O365	Microsoft 365 Apps, Office 2019, and Office LTSC 2021	2	Elevation of Privilege	Important	2	■■□□	
MS23-10-SO8	Server 2012	60	Remote Code Execution	Critical	1	■■■■	Known Exploited and Publicly Disclosed: CVE-2023-36563
MS23-10-SO81	Server 2012 R2	61	Remote Code Execution	Critical	1	■■■■	Known Exploited and Publicly Disclosed: CVE-2023-36563
MS23-10-SQL	SQL Server 2014, 2016, 2017, 2019 & 2022	5	Remote Code Execution	Important	2	■■□□	
MS23-10-W10	Windows 10, Server 2016, Server 2019, Server 2022, Edge Chromium and IE 11	80	Remote Code Execution	Critical	1	■■■■	Known Exploited: CVE-2023-44487 Known Exploited and Publicly Disclosed: CVE-2023-36563
MS23-10-W11	Windows 11 and Edge Chromium	75	Remote Code Execution	Critical	1	■■■■	Known Exploited: CVE-2023-44487 Known Exploited and Publicly Disclosed: CVE-2023-36563