ivanti Patch Tuesday

September 12, 2023

	Bulletin	Critical	Important
Adobe	1 Bulletin	1 Critical	0 Important
Google	1 Bulletin	1 Critical	0 Important
Microsoft	13 Bulletins	2 Critical	11 Important
moz://a	1 Bulletin	1 Critical	0 Important

September 2023 Patch Tuesday has a lot of activity and the theme this month is "Everyone has a zero-day release!" Microsoft has resolved 63 total vulnerabilities including two exploited Zero-days (CVE-2023-36761 and CVE-2023-36802). Google Chrome resolved one Zero-day vulnerability (CVE-2023-4863) on September 11 which is also included in the Microsoft Edge Chromium release. Adobe resolved a Zero-day vulnerability in Acrobat and Reader (APSB23-34 CVE-2023-26369) on September 12. Apple resolved two Zero-days on September 7 (CVE-2023-41064 and CVE-2023-41061). There aren't any recent zero-day vulnerabilities on the Linux side, but there are three recent vulnerabilities that are affecting some core capabilities in the Linux Kernel that warrant some attention.

Adobe Bulletins	Affected products	CVE count	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
APSB23-34	Adobe Acrobat and Reader	1	Remote Code Execution	Critical	1	🟧🟧🟥🟥	Known Exploited: CVE-2023-26369

Google Bulletins	Affected products	CVE count	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
Chrome-230912	Chrome	1	Remote Code Execution	Critical	1	🟧🟧🟥🟥	Known Exploited: CVE-2023-4863

Microsoft Bulletins	Affected products	CVE count	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
MS23-09-EXCH	Microsoft Exchange Server 2016 - 2019	5	Remote Code Execution	Important	2	🟧🟧⬜⬜	
MS23-09-IE	Internet Explorer 11	1	Security Feature Bypass	Important	2	🟧🟧⬜⬜	
MS23-09-MR8	Server 2012 and IE	12	Denial of Service	Important	2	🟧🟧⬜⬜	
MS23-09-MR81	Server 2012 R2 and IE	13	Security Feature Bypass	Important	2	🟧🟧⬜⬜	
MS23-09-MRNET	.NET Framework 2.0-4.8.1	5	Remote Code Execution	Important	2	🟧🟧⬜⬜	
MS23-09-OFF	Excel 2013 & 2016, Office 2013 & 2016, Office Online Server, Outlook 2016,Office 2019 & LTSC 2021 for Mac, and Word 2103 & 2016	6	Remote Code Execution	Important	1	🟧🟧🟥🟥	Known Exploited and Publicly Disclosed: CVE-2023-36761
MS23-09-O365	Microsoft 365 Apps, Office 2019, and Office LTSC 2021	7	Remote Code Execution	Important	1	🟧🟧🟥🟥	Known Exploited and Publicly Disclosed: CVE-2023-36761
MS23-09-SO8	Server 2012	12	Denial of Service	Important	2	🟧🟧⬜⬜	
MS23-09-SO81	Server 2012 R2	13	Security Feature Bypass	Important	2	🟧🟧⬜⬜	
MS23-09-SONET	.NET Framework 2.0-4.8.1	5	Remote Code Execution	Important	2	🟧🟧⬜⬜	
MS23-09-SPT	Sharepoint Server 2016- 2019	2	Remote Code Execution	Important	2	🟧🟧⬜⬜	
MS23-09-W10	Windows 10, Server 2016, Server 2019, Server 2022, Edge Chromium and IE 11	20	Remote Code Execution	Critical	1	🟧🟧🟥🟥	Known Exploited: CVE-2023-4863 and CVE-2023-36802
MS23-09-W11	Windows 11 and Edge Chromium	19	Remote Code Execution	Critical	1	🟧🟧🟥🟥	Known Exploited: CVE-2023-4863 and CVE-2023-36802

Mozilla Bulletins	Affected products	CVE count	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
MFSA-2023-40	Firefox, Firefox ESR, Thunderbird	1	Remote Code Execution	Critical	1	🟧🟧🟥🟥	Known Exploited: CVE-2023-4863

ivanti