ivanti Patch Tuesday

April 11, 2023

Adobe — 1 Bulletin | 1 Critical | 0 Important

Microsoft — 9 Bulletins | 6 Critical | 3 Important

mozilla — 2 Bulletins | 2 Critical | 0 Important

We enter into this April Patch Tuesday on the heels of a CISA advisory and updates from Apple (released on April 7th and 10th) for macOS, iPad OS, iOS and Safari resolving two Zero Day exploits (CVE-2023-28205 and CVE-2023-28206). Microsoft has released updates resolving 97 new CVEs with one new confirmed exploited vulnerability (CVE-2023-28252) resolved in the Windows OS update this month. Microsoft has updated the affected products list for CVE-2013-3900, a previously resolved vulnerability that has been confirmed to be exploited. Third-party updates from Mozilla and Adobe have also released and Oracle's CPU release is coming on April 18th, which will be followed by a stream of Java alternatives being updated through the rest of the month.

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

Adobe Bulletin	Affected products	CVE count	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
APSB23-24	Acrobat and Reader	16	Remote Code Execution	Critical	1		
Microsoft Bulletins	**Affected products**	**CVE count**	**Impact**	**Vendor severity**	**Ivanti priority**	**Threat risk**	**Disclosures & Exploits**
MS23-04-MR8	Server 2012 and IE	62	Remote Code Execution	Critical	1		Known Exploited and Publicly Disclosed: CVE-2023-3900 (re-issued) Known Exploited: CVE-2023-28252
MS23-04-MR81	Server 2012 R2 and IE	62	Remote Code Execution	Critical	1		Known Exploited and Publicly Disclosed: CVE-2023-3900 (re-issued) Known Exploited: CVE-2023-28252
MS23-04-OFF	Office 2019 & Office LTSC 2021 for Mac, Office Publisher 2013 - 2019	4	Remote Code Execution	Important	2		
MS23-04-O365	Microsoft 365 Apps, Office 2019, and Office LTSC 2021	4	Remote Code Execution	Important	2		
MS23-04-SO8	Server 2012	62	Remote Code Execution	Critical	1		Known Exploited and Publicly Disclosed: CVE-2023-3900 (re-issued) Known Exploited: CVE-2023-28252
MS23-04-SO81	Server 2012 R2	62	Remote Code Execution	Critical	1		Known Exploited and Publicly Disclosed: CVE-2023-3900 (re-issued) Known Exploited: CVE-2023-28252
MS23-04-SPT	Sharepoint Server 2013 - 2019	1	Spoofing	Important	2		
MS23-04-W10	Windows 10, Server 2016, Server 2019, Server 2022, Edge Chromium and IE 11	74	Remote Code Execution	Critical	1		Known Exploited and Publicly Disclosed: CVE-2023-3900 (re-issued) Known Exploited: CVE-2023-28252 Publicly Disclosed: CVE-2022-43552 (re-issued)
MS23-04-W11	Windows 11 and Edge Chromium	59	Remote Code Execution	Critical	1		Known Exploited and Publicly Disclosed: CVE-2023-3900 (re-issued) Known Exploited: CVE-2023-28252 Publicly Disclosed: CVE-2022-43552 (re-issued)
Mozilla Bulletins	**Affected products**	**CVE count**	**Impact**	**Vendor severity**	**Ivanti priority**	**Threat risk**	**Disclosures & Exploits**
MFSA 2023-13	Firefox 112	22	Remote Code Execution	Critical	1		
MFSA 2023-14	Firefox ESR 102.10	13	Remote Code Execution	Critical	1		

ivanti