ivanti Patch Tuesday

July 11, 2023

	Bulletins	Critical	Important
Microsoft	10	7	3
moz://a	2	0	0

Microsoft resolved 130 new CVEs, updated 9 CVEs, and released\updated 3 Advisories this month. There are 6 confirmed Zero Day Exploits this month and another with functional exploit code. The OS and Office updates are going to be your priority this month and will take care of the majority of the risk, but CVE-2023-36884 is a configuration-only mitigation currently so another update may come in the near future. There are some operational changes in NetLogon and Kerberos stepping up enforcement from a couple of CVEs resolved in 2022 that you will want to be aware of. For more details check out our complete writeup in this months Patch Tuesday Blog: ivanti.com/blog/july-2023-patch-tuesday

Microsoft Bulletins	Affected products	CVE count	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
MS23-07-IE	Internet Explorer 11	1	Elevation of Privilege	Important	1	■■■■	Known Exploited: CVE-2023-32046
MS23-07-MR8	Server 2012 and IE	69	Remote Code Execution	Critical	1	■■■■	Known Exploited and Publicly Disclosed: *CVE-2023-36884, CVE-2023-24932 (re-issued) Known Exploited: CVE-2023-32046, CVE-2023-36874 *Currently Mitigated by Configuration
MS23-07-MR81	Server 2012 R2 and IE	71	Remote Code Execution	Critical	1	■■■■	Known Exploited and Publicly Disclosed: *CVE-2023-36884, CVE-2023-24932 (re-issued) Known Exploited: CVE-2023-32046, CVE-2023-36874 *Currently Mitigated by Configuration
MS23-07-OFF	Excel 2013 & 2016, Outlook 2103 & 2016, Office Online Server, Office 2019 & LTSC 2021 for Mac, and Microsoft Word 2013 & 2016	10	Remote Code Execution	Important	1	■■■■	Known Exploited and Publicly Disclosed: *CVE-2023-36884 Known Exploited: CVE-2023-35311 *Currently Mitigated by Configuration
MS23-07-O365	Microsoft 365 Apps, Office 2019, and Office LTSC 2021	11	Remote Code Execution	Important	1	■■■■	Known Exploited and Publicly Disclosed: *CVE-2023-36884 Known Exploited: CVE-2023-35311 *Currently Mitigated by Configuration
MS23-07-SO8	Server 2012	69	Remote Code Execution	Critical	1	■■■■	Known Exploited and Publicly Disclosed: *CVE-2023-36884, CVE-2023-24932 (re-issued) Known Exploited: CVE-2023-32046, CVE-2023-36874 *Currently Mitigated by Configuration
MS23-07-SO81	Server 2012 R2	71	Remote Code Execution	Critical	1	■■■■	Known Exploited and Publicly Disclosed: *CVE-2023-36884, CVE-2023-24932 (re-issued) Known Exploited: CVE-2023-32046, CVE-2023-36874 *Currently Mitigated by Configuration
MS23-07-SPT	Sharepoint Server 2016 & 2019, Sharepoint Server Subscription Edition	5	Remote Code Execution	Critical	1	■■■■	
MS23-07-W10	Windows 10, Server 2016, Server 2019, Server 2022, Edge Chromium and IE 11	99	Remote Code Execution	Critical	1	■■■■	Known Exploited and Publicly Disclosed: *CVE-2023-36884, CVE-2023-24932 (re-issued) Known Exploited: CVE-2023-32046, CVE-2023-32049, CVE-2023-36874 *Currently Mitigated by Configuration
MS23-07-W11	Windows 11 and Edge Chromium	84	Remote Code Execution	Critical	1	■■■■	Known Exploited and Publicly Disclosed: *CVE-2023-36884, CVE-2023-24932 (re-issued) Known Exploited: CVE-2023-32046, CVE-2023-32049, CVE-2023-36874 *Currently Mitigated by Configuration
Mozilla Bulletins	**Affected products**	**CVE count**	**Impact**	**Vendor severity**	**Ivanti priority**	**Threat risk**	**Disclosures & Exploits**
MFSA-2023-26	Firefox 115.0.2	1	Denial of Service	High	2	■■□□	
MFSA-2023-26	Firefox ESR 115.0.2	1	Denial of Service	High	2	■■□□	