ivanti PATCH TUESDAY

April 9, 2019

22 New Bulletins

17 User Targeted

2 Zero Days

	Bulletins	Critical	Important	User Targeted
Adobe	4	3	0	3
Microsoft	15	11	4	14
Other	3	3	0	0

For the Ivanti patch product team, the snow is melting and spring is here—and that means it's time for April Patch Tuesday spring cleaning. Let's get our houses in order! Patch what you can, prioritizing Adobe and Microsoft's OS and browsers. Get rid of Wireshark where possible, because that one's serving up the bad this month. And remove Shockwave, too, because it's coming in hot and patching is no longer an option. Exploits are looming there, and that's not good for your IT team feng shui.

	Bulletins	CVE Count	Impact	Vendor Severity	Ivanti Priority	Threat Risk	Notes	User Targeted	Privilege Management Mitigates Impact
Adobe	**AAIR19-3200116** Air	None			2	🟥🟥□□			
	APSB19-17 Acrobat and Reader	21	Remote Code Execution	Critical	1	🟥🟥🟥□		✓	
	APSB19-20 Shockwave	7	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Product is End-of-Lifed	✓	
	APSB19-19 Flash Player	2	Remote Code Execution	Critical	1	🟥🟥🟥□		✓	
Microsoft	**MS19-04-AFP** Flash Player	2	Remote Code Execution	Critical	1	🟥🟥🟥□		✓	
	MS19-04-EX Exchange Server 2010-2019	2	Spoofing	Important	2	🟥🟥□□		✓	
	MS19-04-IE Internet Explorer 9, 10, 11	5	Remote Code Execution	Critical	1	🟥🟥🟥□		✓	✓
	MS19-04-MR2K8 Server 2008	29	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0803, CVE-2019-0859	✓	✓
	MS19-04-MR7 Windows 7, Server 2008 R2 and IE	34	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0803, CVE-2019-0859	✓	✓
	MS19-04-MR8 Server 2012 and IE	36	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0803, CVE-2019-0859	✓	✓
	MS19-04-MR81 Windows 8.1, Server 2012 R2 and IE	36	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0803, CVE-2019-0859	✓	✓
	MS19-04-OFF Excel 2010-2016, Office 2010-2016, Office 2016 and 2019 for Mac	8	Remote Code Execution	Important	2	🟥🟥□□		✓	✓
	MS19-04-O365 Office 365 ProPlus, Office 2019	7	Remote Code Execution	Important	2	🟥🟥□□		✓	✓
	MS19-04-SO2K8 Server 2008	29	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0803, CVE-2019-0859	✓	✓
	MS19-04-SO7 Windows 7 and Server 2008 R2	29	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0803, CVE-2019-0859	✓	✓
	MS19-04-SO8 Server 2012	31	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0803, CVE-2019-0859	✓	✓
	MS19-04-SO81 Windows 8.1 and Server 2012 R2	31	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0803, CVE-2019-0859	✓	✓
	MS19-04-SPT Sharepoint Server 2010-2019	2	Spoofing	Important	2	🟥🟥□□			✓
	MS19-04-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	50	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0803, CVE-2019-0859	✓	✓
Other	**WIRES-092** Wireshark 2.4.14	6	Remote Code Execution	Critical	1	🟥🟥🟥□			
	WIRES-093 Wireshark 2.6.8	6	Remote Code Execution	Critical	1	🟥🟥🟥□			
	WIRES-094 Wireshark 3.0.1	10	Remote Code Execution	Critical	1	🟥🟥🟥□			

For additional analysis and insight visit: **ivanti.com/patch-tuesday**

ivanti