ivanti PATCH TUESDAY

May 14, 2019

20 New Bulletins

15 User Targeted

1 Zero Day

	Bulletins	Critical	Important	User Targeted
Adobe	2	2	0	2
Microsoft	17	13	4	13
VMware	1 Bulletin	0	0	0

Superstition holds you shouldn't buy a broom, wash a blanket, or get married in May. What you should do, though, is patch—and all the more so this May Patch Tuesday! Make quick work of this month's zero day. No need for superstition there, as that one has proven itself a menace via exploits in the wild. Prioritize everything publicly disclosed and patch the Windows vulnerability primed to unleash a WannaCry-like event two years after the original (to the very month, in fact—so maybe there is something to May superstitions after all).

	Bulletins	CVE Count	Impact	Vendor Severity	Ivanti Priority	Threat Risk	Notes	User Targeted	Privilege Management Mitigates Impact
Adobe	**APSB19-18** Acrobat and Reader	84	Remote Code Execution	Critical	1	🟥🟥🟥⬜		●	
	APSB19-26 Flash Player	1	Remote Code Execution	Critical	1	🟥🟥🟥⬜		●	
Microsoft	**MS19-05-AFP** Flash Player	1	Remote Code Execution	Critical	1	🟥🟥🟥⬜		●	
	MS19-05-IE Internet Explorer 9, 10, 11	8	Remote Code Execution	Critical	1	🟥🟥🟥⬜		●	●
	MS19-05-MR2K8 Server 2008	22	Remote Code Execution	Critical	1	🟥🟥🟥⬜		●	●
	MS19-05-MR7 Windows 7, Server 2008 R2 and IE	32	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Publicly Disclosed: CVE-2019-0863 Exploited in Wild: CVE-2019-0863	●	●
	MS19-05-MR8 Server 2012 and IE	32	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Publicly Disclosed: CVE-2019-0863 Exploited in Wild: CVE-2019-0863	●	●
	MS19-05-MR81 Windows 8.1, Server 2012 R2 and IE	32	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Publicly Disclosed: CVE-2019-0863 Exploited in Wild: CVE-2019-0863	●	●
	MS19-05-MRNET .NET Framework 2.0-4.8	4	Denial of Service	Important	2	🟥🟥⬜⬜			
	MS19-05-OFF Office 2010-2016, Office 2016 and 2019 for Mac, Word 2016	4	Remote Code Execution	Critical	1	🟥🟥🟥⬜		●	●
	MS19-05-O365 Office 365 ProPlus, Office 2019	3	Remote Code Execution	Critical	1	🟥🟥🟥⬜		●	
	MS19-05-SO2K8 Server 2008	22	Remote Code Execution	Critical	1	🟥🟥🟥⬜		●	●
	MS19-05-SO7 Windows 7 and Server 2008 R2	24	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Publicly Disclosed: CVE-2019-0863 Exploited in Wild: CVE-2019-0863	●	●
	MS19-05-SO8 Server 2012	24	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Publicly Disclosed: CVE-2019-0863 Exploited in Wild: CVE-2019-0863	●	●
	MS19-05-SO81 Windows 8.1 and Server 2012 R2	24	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Publicly Disclosed: CVE-2019-0863 Exploited in Wild: CVE-2019-0863	●	●
	MS19-05-SONET .NET Framework 2.0-4.8	4	Denial of Service	Important	2	🟥🟥⬜⬜			
	MS19-05-SPT Sharepoint Server 2010-2019	8	Remote Code Execution	Important	2	🟥🟥⬜⬜			
	MS19-05-SQL SQL Server 2017	1	Information Disclosure	Important	2	🟥🟥⬜⬜			
	MS19-05-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	53	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Publicly Disclosed: CVE-2019-0863 Exploited in Wild: CVE-2019-0863	●	●
VMware	**VMSA-2019-0007** VMware Workstation Pro / Player	1	Privilege Escalation	Medium	2	🟥🟥⬜⬜			

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

ivanti