ivanti PATCH TUESDAY

March 12, 2019

16 New Bulletins

12 User Targeted

2 Zero Days

	Bulletin	Critical	Important	User Targeted
Adobe	1	0	0	0
Google	1	1	0	1
Microsoft	14	10	2	11

Unless you've the luck of the Irish—and, really, even if you do—you'll want a rapid start on March Patch Tuesday. The rainbow this month ends in Windows zero days and public disclosures. And, unlike the elusive four-leaf clover, elevation of privilege is popping up all over, so make sure you're reviewing your admin privileges when you patch the vulnerabilities in your environment. As we sign off this month, take note that Chrome will need attention, too, starting with the zero day resolved on March 1. May you be halfway to safety before the hackers know you're vulnerable!

	Bulletins	CVE Count	Impact	Vendor Severity	Ivanti Priority	Threat Risk	Notes	User Targeted	Privilege Management Mitigates Impact
Adobe	APSB19-12 Flash Player	None		Low	3	□□□□	No CVEs reported		
Google	CHROME-247 Chrome	60	Remote Code Execution	Critical	1	🟥🟥🟥□		👤	
Microsoft	MS19-03-AFP Flash Player	None	Defense in Depth	Low	3	□□□□	No CVEs reported		
	MS19-03-IE Internet Explorer 9, 10, 11	12	Remote Code Execution	Critical	1	🟥🟥🟥□		👤	↕
	MS19-03-MR2K8 Server 2008	21	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0808 Publicly Disclosed: CVE-2019-0683, CVE-2019-0754	👤	↕
	MS19-03-MR7 Windows 7, Server 2008 R2 and IE	33	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0808 Publicly Disclosed: CVE-2019-0683, CVE-2019-0754	👤	↕
	MS19-03-MR8 Server 2012 and IE	32	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0797 Publicly Disclosed: CVE-2019-0754	👤	↕
	MS19-03-MR81 Windows 8.1, Server 2012 R2 and IE	32	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0797 Publicly Disclosed: CVE-2019-0754	👤	↕
	MS19-03-OFF Office 2010, Lync Server 2013, Skype Business Server 2015	2	Remote Code Execution	Important	2	🟥🟥□□		👤	
	MS19-03-O365 Office 365 ProPlus, Office 2019	None			3	□□□□	No CVEs reported		
	MS19-03-SO2K8 Server 2008	21	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0808 Publicly Disclosed: CVE-2019-0683, CVE-2019-0754	👤	↕
	MS19-03-SO7 Windows 7 and Server 2008 R2	21	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0808 Publicly Disclosed: CVE-2019-0683, CVE-2019-0754	👤	↕
	MS19-03-SO8 Server 2012	20	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0797 Publicly Disclosed: CVE-2019-0754	👤	↕
	MS19-03-SO81 Windows 8.1 and Server 2012 R2	20	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0797 Publicly Disclosed: CVE-2019-0754	👤	↕
	MS19-03-SPT Sharepoint Server 2013, 2016	1	Tampering	Important	2	🟥🟥□□			↕
	MS19-03-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	55	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Exploited: CVE-2019-0797 Publicly Disclosed: CVE-2019-0754	👤	↕

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

ivanti