ivanti PATCH TUESDAY

January 9, 2018

19 New Bulletins

6 User Targeted

4 Critical

Adobe	1 Bulletin	0 Critical	1 Important	1 User Targeted
Google	1 Bulletin	0 Critical	0 Important	0 User Targeted
Microsoft	14 Bulletins	3 Critical	11 Important	5 User Targeted
Mozilla	1 Bulletin	1 Critical	0 Important	0 User Targeted
Oracle	2 Bulletins	TBA Critical	TBA Important	TBA User Targeted

It's 2018, we're resolved to help you secure your systems against whatever the new year brings, and January Patch Tuesday is bringing it! This month's updates include a fix for a known Office exploit and a host of patches to tackle the Meltdown and Spectre vulnerabilities. About that last bit, though, take note: there is no known malicious use of these vulnerabilities to date. Take the time you need now to put the patches through their paces and get them in place, because this security issue is likely to tempt the bad guys.

	Bulletins	CVE Count	Impact	Vendor Severity	Shavlik Priority	Threat Risk	Notes	User Targeted	Privilege Management Mitigates Impact
Adobe	APSB18-01 Flash Player	1	Information Disclosure	Important	2	🟥🟥⬜⬜		●	
Google	CHROME-213 Chrome						No CVEs reported		
Microsoft	MS18-01-2K8 Server 2008	7	Information Disclosure	Important	2	🟥🟥🟥⬜	Publicly Disclosed: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754		
	MS18-01-IE Internet Explorer 9, 10, 11	5	Remote Code Execution	Critical	1	🟥🟥🟥⬜	Publicly Disclosed: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754	●	⇕
	MS18-01-MR7 Windows 7, Server 2008 R2 and IE	10	Information Disclosure	Important	2	🟥🟥🟥⬜	Publicly Disclosed: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754		
	MS18-01-MR8 Server 2012 and IE	15	Denial of Service	Important	2	🟥🟥🟥⬜	Publicly Disclosed: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754		
	MS18-01-MR81 Windows 8.1, Server 2012 R2 and IE	18	Denial of Service	Important	2	🟥🟥🟥⬜	Publicly Disclosed: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754		
	MS18-01-OFF Office 2007-2016, Excel, Outlook, and Word 2007-2016, Sharepoint Server 2010-2016, Web Apps Server 2010, 2013	19	Remote Code Execution	Critical	1	🟥🟥🟥🟥	Publicly Disclosed: CVE-2018-0819 (Office for Mac only)	●	⇕
	MS18-01-SO7 Windows 7 and Server 2008 R2	10	Information Disclosure	Important	2	🟥🟥🟥⬜	Publicly Disclosed: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754	●	
	MS18-01-SO8 Server 2012	13	Denial of Service	Important	2	🟥🟥🟥⬜	Publicly Disclosed: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754		
	MS18-01-SO81 Windows 8.1 and Server 2012 R2	13	Denial of Service	Important	2	🟥🟥🟥⬜	Publicly Disclosed: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754		
	MS18-01-W10 Windows 10, Server 2016, IE 11, and Edge	21	Remote Code Execution	Critical	1	🟥🟥🟥⬜	Publicly Disclosed: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754	●	⇕
	MS18-01-SQL SQL Server 2016, 2017	3	Information Disclosure	Important	2	🟥🟥⬜⬜	Publicly Disclosed: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754		
	MS18-01-MRNET .Net Framework	2	Security Feature Bypass	Important	2	🟥🟥⬜⬜			
	MS18-01-SONET .Net Framework	2	Security Feature Bypass	Important	2	🟥🟥⬜⬜			
	MS18-01-AFP Flash Player	1	Information Disclosure	Important	2	🟥🟥⬜⬜		●	
Mozilla	FF18-001 Firefox		Remote Code Execution	Critical	1	🟥🟥🟥⬜	Mitigation for Speculative Execution Side-Channel Attacks		
Oracle	Java JRE	TBA	TBA	TBA			Releasing Jan 16th		
	Java JDK	TBA	TBA	TBA			Releasing Jan 16th		

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

ivanti