ivanti PATCH TUESDAY

December 11, 2018

22 New Bulletins

18 User Targeted

3* Zero Days

	Bulletins	Critical	Important	User Targeted
Adobe	3	3	0	3
Microsoft	17	9	8	13
Mozilla	2	2	0	2

This December Patch Tuesday attackers have added a smattering of coal to the gifts in our holiday stockings. You don't want the Flash exploits slipping down the chimney while your back is turned, so make sure Adobe is on your list for maintenance goodies. Attackers could also turn the lights out on your holiday festivities via a Microsoft zero day and public disclosure, so prioritize those CVEs— and make sure you've checked off the other updates before shutting off the lights on 2018. Happy patching and happy holidays!

*Released prior to Patch Tuesday

Bulletins	CVE Count	Impact	Vendor Severity	Ivanti Priority	Threat Risk	Notes	User Targeted	Privilege Management Mitigates Impact
Adobe								
*APSB18-44 Flash Player	1	Remote Code Execution	Critical	1	■■■■	*Released November 20th Exploited in Wild: CVE-2018-15981	●	
*APSB18-42 Flash Player	2	Remote Code Execution	Critical	1	■■■■	*Released December 5th Exploited in Wild: CVE-2018-15982	●	
APSB18-41 Acrobat and Reader	87	Remote Code Execution	Critical	1	■■■□		●	
Microsoft								
*MS18-12-AFP Flash Player	2	Remote Code Execution	Critical	1	■■■■	*Released December 5th Includes Zero Day vulnerabilities CVE-2018-15981, CVE-2018-15982	●	
MS18-12-EX Exchange Server 2016	1	Tampering	Important	2	■■□□			
MS18-12-IE Internet Explorer 9, 10, 11	4	Remote Code Execution	Critical	1	■■■□		●	●
MS18-12-MR2K8 Server 2008	8	Elevation of Privilege	Important	1	■■■■	Exploited in Wild: CVE-2018-8611	●	
MS18-12-MR7 Windows 7, Server 2008 R2 and IE	13	Remote Code Execution	Critical	1	■■■■	Exploited in Wild: CVE-2018-8611	●	●
MS18-12-MR8 Server 2012 and IE	13	Remote Code Execution	Critical	1	■■■■	Exploited in Wild: CVE-2018-8611	●	●
MS18-12-MR81 Windows 8.1, Server 2012 R2 and IE	13	Remote Code Execution	Critical	1	■■■■	Exploited in Wild: CVE-2018-8611	●	●
MS18-12-MR81 .NET 3.5-4.7.2	2	Remote Code Execution	Critical	1	■■■□	Publicly Disclosed: CVE-2018-8517		●
MS18-12-OFF Excel 2010-2016, Office 2010-2016, Office 2016 and 2019 for macOS, Outlook 2010-2016, PowerPoint 2010-2016	7	Remote Code Execution	Important	2	■■□□		●	●
MS18-12-O365 Office 365 ProPlus, Office 2019	6	Remote Code Execution	Important	2	■■□□		●	●
MS18-12-SO2K8 Server 2008	8	Elevation of Privilege	Important	1	■■■■	Exploited in Wild: CVE-2018-8611	●	
MS18-12-S07 Windows 7 and Server 2008 R2	9	Elevation of Privilege	Important	1	■■■■	Exploited in Wild: CVE-2018-8611	●	
MS18-12-S08 Server 2012	9	Elevation of Privilege	Important	1	■■■■	Exploited in Wild: CVE-2018-8611	●	
MS18-12-SO81 Windows 8.1 and Server 2012 R2	9	Remote Code Execution	Critical	1	■■■■	Exploited in Wild: CVE-2018-8611	●	
MS18-12-SONET .NET 3.5-4.7.2	2	Remote Code Execution	Critical	1	■■■□	Publicly Disclosed: CVE-2018-8517		●
MS18-12-SPT Sharepoint Server 2010-2019	4	Remote Code Execution	Important	2	■■□□			●
MS18-12-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	23	Remote Code Execution	Critical	1	■■■■	Exploited in Wild: CVE-2018-8611	●	●
Mozilla								
2018-29 Firefox 64	11	Remote Code Execution	Critical	1	■■■□		●	
2018-30 Firefox ESR 60.4	6	Remote Code Execution	Critical	1	■■■□		●	

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

ivanti