ivanti PATCH TUESDAY

September 11, 2018

21 New Bulletins

17 User Targeted

1 Zero Day

	Bulletin	Critical	Important	User Targeted
Adobe	1 Bulletin	0 Critical	1 Important	1 User Targeted
Google	1 Bulletin	1 Critical	0 Important	1 User Targeted
Microsoft	16 Bulletins	13 Critical	3 Important	15 User Targeted
Other	3 Bulletins	0 Critical	0 Important	0 User Targeted

Across the globe the season is changing, but for September Patch Tuesday the forecast is much as it was last month—another zero day, some public disclosures, a light smattering of third-party updates, and 60+ vulnerabilities resolved by Microsoft. Déjà vu! Also part of our regular patch weather pattern these days, we're reporting cases of elevation of privilege among the CVEs. So, as we say in this part of the world, "rinse and repeat" with your security procedures: 1) patch in order of criticality, and 2) make sure you have a multi-layered security solution in place.

	Bulletins	CVE Count	Impact	Vendor Severity	Ivanti Priority	Threat Risk	Notes	User Targeted	Privilege Management Mitigates Impact
Adobe	**APSB18-31** Flash Player	1	Privilege Escalation	Important	2				
Google	**Chrome-234** Chrome	2	Remote Code Execution	Critical	1				
Microsoft	**MS18-09-AFP** Flash Player	1	Privilege Escalation	Important	2				
	MS18-09-IE Internet Explorer 9, 10, 11	6	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2018-8457		
	MS18-09-MR2K8 Server 2008	17	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440		
	MS18-09-MR7 Windows 7, Server 2008 R2 and IE	24	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475, CVE-2018-8457		
	MS18-09-MR8 Server 2012 and IE	25	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475, CVE-2018-8457		
	MS18-09-MR81 Windows 8.1, Server 2012 R2 and IE	28	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475, CVE-2018-8457		
	MS18-09-MRNET .NET 2.0-4.7.2	1	Remote Code Execution	Critical	1				
	MS18-09-OFF Excel 2010-2016, Office 2016, Word 2013-2016	5	Remote Code Execution	Important	2				
	MS18-09-O365 Office 2016	4	Remote Code Execution	Critical	1				
	MS18-09-SO2K8 Server 2008	17	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475		
	MS18-09-SO7 Windows 7 and Server 2008 R2	18	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475		
	MS18-09-SO8 Server 2012	19	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475		
	MS18-09-SO81 Windows 8.1 and Server 2012 R2	22	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475		
	MS18-09-SONET .NET 2.0-4.7.2	1	Remote Code Execution	Critical	1				
	MS18-09-SPT Sharepoint Server 2013, 2016	3	Elevation of Privilege	Important	2				
	MS18-09-W10 Windows 10, Server 2016, IE 11, and Edge	49	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475, CVE-2018-8457		
Other	**AAIR18-310096** Air				3		Non-Security		
	TOMCAT-118 Tomcat 9.0.12				3		Non-Security		
	TOMCAT-119 Tomcat 8.5.34				3		Non-Security		

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

ivanti