




































 Publicly Disclosed  Zero Day	Microsoft 	14 Bulletins	6 Critical	8 Important	7 User Targeted
	Adobe 	2 Bulletin	1 Critical	0 Important	1 User Targeted
	Google 	1 Bulletin	1 Critical	0 Important	1 User Targeted

While the results of today's US presidential election may be out of your hands, you can still impact the outcome of Patch Tuesday on your environment. You can't buy votes for your favorite candidate, but you can buy yourself some time by implementing privilege management and application control. Reduce the risk of threats that could target your users before patches get applied.



	Bulletins	CVE Count	Impact	Vendor Severity	Shavlik Priority	Threat Risk	User Targeted	Privilege Management Mitigates Impact	Notes
 Microsoft	MS16-129 Edge	17	Remote Code Execution	Critical	1				Publicly Disclosed: CVE-2016-7199, CVE-2016-7209
	MS16-130 Windows	3	Remote Code Execution	Critical	1				
	MS16-131 Windows	1	Remote Code Execution	Critical	1				
	MS16-132 Windows	4	Remote Code Execution	Critical	1				Exploited CVE-2016-7256
	MS16-133 Office, SharePoint, Office Web Apps	12	Remote Code Execution	Important	2				
	MS16-134 Windows	10	Elevation of Privilege	Important	2				
	MS16-135 Windows	5	Elevation of Privilege	Important	1				Publicly Disclosed: CVE-2016-7255, Exploited CVE-2016-7255
	MS16-136 SQL	6	Elevation of Privilege	Important	2				
	MS16-137 Windows	3	Elevation of Privilege	Important	2				
	MS16-138 Windows	4	Elevation of Privilege	Important	2				
	MS16-139 Windows	1	Elevation of Privilege	Important	2				
	MS16-140 Windows	1	Security Feature Bypass	Important	2				
	MS16-141 Flash Player	9	Remote Code Execution	Critical	1				
	MS16-142 Internet Explorer	7	Remote Code Execution	Critical	1				Publicly Disclosed CVE-2016-7199
 Adobe	APSB16-37 Flash Player	9	Remote Code Execution	Critical	1				
	APSB16-35 Connect	1	Remote Code Execution	Low	3				
 Google	CHROME-185 Chrome	TBA	Remote Code Execution	Critical	1				Includes latest Flash Plug-In Support

For additional analysis and insight visit: www.shavlik.com/patch-tuesday