

May 8, 2018

18
New Bulletins

14
User Targeted

2
Zero Day

Adobe



1

Bulletin

1

Critical

0

Important

1

User Targeted

Microsoft



17

Bulletins

11

Critical

5

Important

13

User Targeted

They say May brings flowers, but we're getting more Patch Tuesday showers this month. Get ready to defend against a heavy downpour of CVEs, including zero-days and other critical vulnerabilities. Rain is also in the forecast in the guise of public disclosures, so patch the holes in those systems before the deluge can begin. And finally? Some of this inclement weather is designed to grant the necessary access rights—so, remember, even with privilege management in place, you need to properly layer on security to keep the storms at bay.

	Bulletins	CVE Count	Impact	Vendor Severity	Shavlik Priority	Threat Risk	Notes	User Targeted	Privilege Management Mitigates Impact
Adobe	APSB18-16 Flash Player	1	Remote Code Execution	Critical	1				
Microsoft	MS18-05-2K8 Server 2008	10	Remote Code Execution	Critical	1		Exploited in Wild CVE-2018-8174, CVE-2018-8120		
	MS18-05-AFP Flash Player	1	Remote Code Execution	Critical	1				
	MS18-05-EX Exchange Server 2010-2016	5	Remote Code Execution	Critical	1				
	MS18-05-IE Internet Explorer 9, 10, 11	9	Remote Code Execution	Critical	1				
	MS18-05-MR7 Windows 7, Server 2008 R2 and IE	20	Remote Code Execution	Critical	1		Exploited in Wild CVE-2018-8174, CVE-2018-8120		
	MS18-05-MR8 Server 2012 and IE	19	Remote Code Execution	Critical	1		Exploited in Wild CVE-2018-8174		
	MS18-05-MR81 Windows 8.1, Server 2012 R2 and IE	20	Remote Code Execution	Critical	1		Exploited in Wild CVE-2018-8174		
	MS18-05-MRNET .NET 2.0-4.7.1	2	Security Feature Bypass	Important	2				
	MS18-05-0365 Office 2016	7	Remote Code Execution	Important	2				
	MS18-05-OFF Office 2010-2016, Excel 2010-2016, Word 2010-2016, Web Apps and Project Server, Office 2016 for Mac	10	Remote Code Execution	Important	2				
	MS18-05-S07 Windows 7 and Server 2008 R2	11	Remote Code Execution	Critical	1		Exploited in Wild CVE-2018-8174, CVE-2018-8120		
	MS18-05-S08 Server 2012	10	Remote Code Execution	Critical	1		Exploited in Wild CVE-2018-8174		
	MS18-05-S081 Windows 8.1 and Server 2012 R2	11	Remote Code Execution	Critical	1		Exploited in Wild CVE-2018-8174		
	MS18-05-SONET .NET 2.0-4.7.1	2	Security Feature Bypass	Important	2				
	MS18-05-SPT Sharepoint Server 2010-2016	5	Remote Code Execution	Important	2				
	MS18-05-W10 Windows 10, Server 2016, IE 11, and Edge	43	Remote Code Execution	Critical	1		Exploited in Wild CVE-2018-8174, Publicly Disclosed CVE-2018-8141, CVE-2018-8170		
	PBID-031 PowerBI						Non-Security		

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