ivanti PATCH TUESDAY

July 10, 2018

20 New Bulletins

8 Critical

13 User Targeted

	Bulletins	Critical	Important	User Targeted
Adobe	2	2	0	2
Apple	3	0	0	1
Microsoft	15	6	9	10

Whether you're smack dab in the middle of the "dog days" of summer or entering the coldest month of your year, Patch Tuesday is, as they say, as constant as the weather. The same goes for patch management: This July we recommend you prioritize the Adobe and Microsoft updates and roll out all other patches in a timely fashion. Keep an eye out for Oracle updates too. And whether it's hot or cold where you are, don't forget to layer on security so the apps you can't patch don't expose your business to the elements.

	Bulletins	CVE Count	Impact	Vendor Severity	Shavlik Priority	Threat Risk	Notes	User Targeted	Privilege Management Mitigates Impact
Adobe	APSB18-24 Flash Player	2	Remote Code Execution	Critical	1				
	APSB18-21 Acrobat and Reader	104	Remote Code Execution	Critical	1				
Apple	AI18-005 iTunes	14	Remote Code Execution		2		Severity not specified by vendor		
	ICLOUD-012 iCloud	14	Remote Code Execution		2		Severity not specified by vendor		
	AMDS-021 Apple Mobile Device Support	N/A	N/A	N/A	2		Severity not specified by vendor		
Microsoft	MS18-07-2K8 Server 2008	7	Security Feature Bypass	Important	1		Publicly disclosed: CVE-2018-8314		
	MS18-07-IE Internet Explorer 9, 10, 11	6	Remote Code Execution	Critical	1				
	MS18-07-MR7 Windows 7, Server 2008 R2 and IE	13	Remote Code Execution	Critical	1		Publicly disclosed: CVE-2018-8314		
	MS18-07-MR8 Server 2012 and IE	14	Remote Code Execution	Critical	1		Publicly disclosed: CVE-2018-8313, CVE-2018-8314		
	MS18-07-MR81 Windows 8.1, Server 2012 R2 and IE	14	Remote Code Execution	Critical	1		Publicly disclosed: CVE-2018-8313, CVE-2018-8314		
	MS18-07-MRNET .NET 3.5-4.7.2	4	Remote Code Execution	Important	2				
	MS18-07-OFF Office 2010-2016, Access 2013-2016, Word 2010-2016, Lync 2013, Skype for Business 2016	5	Remote Code Execution	Important	2				
	MS18-07-O365 Office 2016	3	Remote Code Execution	Important	2				
	MS18-07-S07 Windows 7 and Server 2008 R2	7	Security Feature Bypass	Important	1		Publicly disclosed: CVE-2018-8314		
	MS18-07-S08 Server 2012	8	Security Feature Bypass	Important	1		Publicly disclosed: CVE-2018-8313, CVE-2018-8314		
	MS18-07-S081 Windows 8.1 and Server 2012 R2	8	Security Feature Bypass	Important	1		Publicly disclosed: CVE-2018-8313, CVE-2018-8314		
	MS18-07-SONET .NET 3.5-4.7.2	4	Remote Code Execution	Important	2				
	MS18-07-W10 Windows 10, Server 2016, IE 11, and Edge	31	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2018-8278, CVE-2018-8313, CVE-2018-8314		
	MS18-07-SPT Sharepoint Server 2013, 2016	3	Remote Code Execution	Important	2				
	MS18-07-AFP Flash Player	2	Remote Code Execution	Critical	1				

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

ivanti