ivanti | Patch Tuesday

September 10, 2019

18 New Bulletins

13 Critical

16 User Targeted

	Bulletin	Critical	Important	User Targeted
Adobe	1 Bulletin	1	0	1
Microsoft	17 Bulletins	12	5	15

Here's your guide to harvesting September's software updates to enhance security online. Start with Microsoft to update the zero-day vulnerabilities in the operating systems, and move on to SharePoint. Next, Office, Exchange and .NET are ripe for patching. On the third-party side, Adobe Flash is back with a security update including 2 CVEs. And, keep an eye out for the Google Chrome release available later today or tomorrow. So pick your patches now to boost your yield, and avoid missing out on new features in addition to security fixes.

	Bulletins	CVE Count	Impact	Vendor Severity	Ivanti Priority	Threat Risk	Notes	User Targeted	Privilege Management Mitigates Impact
Adobe	**APSB19-46** Flash Player	**2**	Remote Code Execution	Critical	**1**			✓	
Microsoft	**MS19-09-AFP** Adobe Flash Player	**2**	Remote Code Execution	Critical	**1**			✓	
	MS19-09-IE Internet Explorer 9, 10, 11	**4**	Remote Code Execution	Critical	**1**			✓	✓
	MS19-09-EXCH Exchange Server 2016 and 2019	**2**	Spoofing	Important	**2**			✓	
	MS19-09-MR2K8 Server 2008 and IE 9	**29**	Remote Code Execution	Critical	**1**		Exploited: CVE-2019-1214, CVE-2019-1215 Publicly Disclosed: CVE-2019-1235	✓	✓
	MS19-09-MR7 Windows 7, Server 2008 R2 and IE	**36**	Remote Code Execution	Critical	**1**		Exploited: CVE-2019-1214, CVE-2019-1215 Publicly Disclosed: CVE-2019-1235	✓	✓
	MS19-09-MR8 Server 2012 and IE	**33**	Remote Code Execution	Critical	**1**		Exploited: CVE-2019-1214, CVE-2019-1215 Publicly Disclosed: CVE-2019-1235	✓	✓
	MS19-09-MR81 Windows 8.1, Server 2012 R2 and IE	**37**	Remote Code Execution	Critical	**1**		Exploited: CVE-2019-1214, CVE-2019-1215 Publicly Disclosed: CVE-2019-1235	✓	✓
	MS19-09-MRNET .NET Framework 3.5-4.8	**1**	Elevation of Privilege	Important	**2**		Server 2012 and newer		
	MS19-09-OFF Excel 2010-2016, Office 2010 and 2013, Office 2016 for Mac, Project 2010-2016	**4**	Remote Code Execution	Important	**2**			✓	✓
	MS19-09-O365 Office 365 ProPlus, Office 2019	**4**	Remote Code Execution	Important	**2**			✓	✓
	MS19-09-SO2K8 Server 2008	**26**	Remote Code Execution	Critical	**1**		Exploited: CVE-2019-1214, CVE-2019-1215 Publicly Disclosed: CVE-2019-1235	✓	✓
	MS19-09-SO7 Windows 7 and Server 2008 R2	**32**	Remote Code Execution	Critical	**1**		Exploited: CVE-2019-1214, CVE-2019-1215 Publicly Disclosed: CVE-2019-1235	✓	✓
	MS19-09-SO8 Server 2012	**29**	Remote Code Execution	Critical	**1**		Exploited: CVE-2019-1214, CVE-2019-1215 Publicly Disclosed: CVE-2019-1235	✓	✓
	MS19-09-SO81 Windows 8.1 and Server 2012 R2	**33**	Remote Code Execution	Critical	**1**		Exploited: CVE-2019-1214, CVE-2019-1215 Publicly Disclosed: CVE-2019-1235	✓	✓
	MS19-09-SONET .NET Framework 3.5-4.8	**1**	Elevation of Privilege	Important	**2**		Server 2012 and newer		
	MS19-09-SPT Sharepoint Server 2010-2019	**7**	Remote Code Execution	Critical	**1**			✓	✓
	MS19-09-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	**57**	Remote Code Execution	Critical	**1**		Exploited: CVE-2019-1214, CVE-2019-1215 Publicly Disclosed: CVE-2019-1235, CVE-2019-1253, CVE-2019-1294	✓	✓

For more information visit: **ivanti.com/patch-tuesday**