ivanti PATCH TUESDAY

February 12, 2019

19
New Bulletins

19
User Targeted

1
Zero Day

	Bulletins	Critical	Important	User Targeted
Adobe	2	1	1	2
Microsoft	17	11	6	17

The average spent on Valentine's Day is a topic that's been making the rounds on social media. It's generated shock and awe—but it's nothing compared to the damage one exploited vulnerability can unleash on your organization. So, let's keep the money in February flowing into flower stores and candlelit dinners, rather than into the pockets of those we'd never choose to date.
For February the men (and women) of Patch Tuesday recommend you lavish attention upon Microsoft. Patch the exploited zero day, public disclosures, and privilege escalation vulnerability. Also, make time for the ever-popular target, Adobe. Because nothing leaves a worse taste in your mouth than a breach you could have prevented—unless, perhaps, it's those chalky conversation hearts.

	Bulletins	CVE Count	Impact	Vendor Severity	Ivanti Priority	Threat Risk	Notes	User Targeted	Privilege Management Mitigates Impact
Adobe	**APSB19-06** Flash Player	1	Information Disclosure	Important	2				
	APSB19-07 Acrobat and Reader	71	Remote Code Execution	Critical	1				
Microsoft	**MS19-02-AFP** Flash Player	1	Information Disclosure	Important	2				
	MS19-02-EX Exchange Server 2010-2019	2	Elevation of Privilege	Important	1		Publicly Disclosed: CVE-2019-0686, CVE-2019-0724		
	MS19-02-IE Internet Explorer 9, 10, 11	3	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2019-0676		
	MS19-02-IE Server 2008	24	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2019-0676 Publicly Disclosed: CVE-2019-0636		
	MS19-02-IE Windows 7, Server 2008 R2 and IE	27	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2019-0676 Publicly Disclosed: CVE-2019-0636		
	MS19-02-MR8 Server 2012 and IE	28	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2019-0676 Publicly Disclosed: CVE-2019-0636		
	MS19-02-MR81 Windows 8.1, Server 2012 R2 and IE	28	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2019-0676 Publicly Disclosed: CVE-2019-0636		
	MS19-02-MRNET .NET Framework 2.0-4.7.2	2	Remote Code Execution	Important	2				
	MS19-02-OFF Excel 2010-2016, Office 2010-2016, Office 2016 for macOS	7	Remote Code Execution	Important	2				
	MS19-02-O365 Office 365 ProPlus, Office 2019	6	Remote Code Execution	Important	2				
	MS19-02-SO2K8 Server 2008	24	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2019-0636		
	MS19-02-SO7 Windows 7 and Server 2008 R2	24	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2019-0636		
	MS19-02-SO8 Server 2012	25	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2019-0636		
	MS19-02-SO81 Windows 8.1 and Server 2012 R2	25	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2019-0636		
	MS19-02-SONET .NET Framework 2.0-4.7.2	2	Remote Code Execution	Important	2				
	MS19-02-SPT Sharepoint Server 2010-2019	4	Remote Code Execution	Critical	1				
	MS19-02-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	52	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2019-0676 Publicly Disclosed: CVE-2019-0636		

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

ivanti