TLP: WHITE

Advisory Alert

Alert No: AAA190301 Date: 13-Mar-19 12:31 PM

Classification	The Alert	: Public Circulation Permitted

Security Updates for 13th March 2019

Overview	High	Drupal	▪ Remote Code Execution Vulnerability
		WinRAR	▪ Remote Code Execution Vulnerability
		Cisco Router	▪ Remote Code Execution Vulnerability
		Microsoft	▪ Multiple Vulnerabilities
	Medium	OpenSSL	▪ Vulnerability to Extract Sensitive Information
	Low	Cisco Webex	▪ Command Injection Vulnerability
		Adobe Acrobat , Reader, & Digital Editions	▪ Multiple Vulnerabilities
		Microsoft Internet Information Services	▪ DoS Attack Vulnerability

Description / Impact	Drupal	• Drupal has released a security advisory on a highly critical vulnerability which an attacker could use to perform remote code execution on affected systems. • Affected Products: Drupal 7 and 8 Core • Officially Acknowledged by the Vendor: Yes
	WinRAR	• A third-party library used by WinRAR containing a vulnerability could allow an attacker to perform a remote code execution when a victim opens a specially crafted compressed archive file. • Affected Products: All versions older than v5.70 • Officially Acknowledged by the Vendor: Yes
	Cisco Router	• Cisco has released an advisory relating to RV110W, RV130W and RV215W Routers, where a remote attacker can perform a remote command execution through these routers' management interface. • Affected Products: All releases of RV110W, RV130W and RV215W • Officially Acknowledged by the Vendor: Yes
	Microsoft	• Microsoft has released updates to address multiple vulnerabilities in Microsoft software. Most severe vulnerability could allow for code execution • Affected Products: Multiple products and versions • Officially Acknowledged by the Vendor: Yes
	OpenSSL	• A security advisory has been released by OpenSSL on a vulnerability which an attacker could exploit t gather sensitive information. • Affected Products: Versions 1.0.2–1.0.2q • Officially Acknowledged by the Vendor: No
	Cisco Webex	• Cisco has released an advisory of a vulnerability which an attacker could use to perform a command injection on Cisco Webex Meetings desktop app and Cisco Webex productivity tools. • Affected Products: Cisco Webex Meetings prior to 33.6.6 / Cisco Webex Productivity tool Releases 32.6.0 and later prior to 33.0.7 • Officially Acknowledged by the Vendor: No
	Adobe Acrobat and Reader & Digital Editions	• Adobe has released a security updates for multiple security vulnerabilities of high criticality on several products that an attacker can use to perform malicious activities. • Affected Products: Multiple products and versions • Officially Acknowledged by the Vendor: Yes
	Microsoft Internet Information Services	• Microsoft has issued a security alert of a denial of service (DoS) flaw related to their Internet Information Services (IIS), windows-based web services. An attacker could use this vulnerability to cause a severe spike in CPU utilization by sending a specially crafted HTTP/2 request. • Affected Products: Versions Windows 10 versions 1607, 1703, 1709, 1803 and Windows Server 2016 • Officially Acknowledged by the Vendor: Yes
Additional Information	Visit the links below and follow the instructions given by respective vendors.	
	Drupal	• https://www.drupal.org/sa-core-2019-003
	WinARA	• https://www.win-rar.com/whatsnew.html?&L=0
	Cisco Router	• https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-rmi-cmd-ex
	Microsoft	• https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/ac45e477-1019-e911-a98b-000d3a33a34d
	OpenSSL	• https://www.openssl.org/news/secadv/20190226.txt
	Cisco Webex	• https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-wmda-cmdinj
	Adobe Acrobat and Reader	• https://helpx.adobe.com/security/products/acrobat/apsb19-13.html • https://helpx.adobe.com/security/products/Digital-Editions/apsb19-16.html
	Microsoft Internet Information Services	• https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190005#ID0EMGAC
Disclaimer	The information provided herein is on "as is" basis, without warranty of any kind.	