PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Linux kernel 4.19 and Earlier Use-After-Free Vulnerability - CVE-2018-18559	In the Linux kernel through 4.19, a use-after-free can occur due to a race condition between fanout_add from setsockopt and bind on an AF_PACKET socket. This issue exists because of the 15fe076edea787807a7cdc168df832544b58eba6 incomplete fix for a race condition. The code mishandles a certain multithreaded case involving a packet_do_bind unregister action followed by a packet_notifier register action. Later, packet_release operates on only one of the two applicable linked lists. The attacker can achieve Program Counter control.	Version(s): <= 4.19	Published - Oct 22, 2018 CVE- 2018-170218559 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-185593 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18559
Splunk Enterprise and Splunk Light Remote DoS Vulnerability - CVE-2018-7432	Splunk Enterprise 6.2.x before 6.2.14, 6.3.x before 6.3.10, 6.4.x before 6.4.7, and 6.5.x before 6.5.3; and Splunk Light before 6.6.0 allow remote attackers to cause a denial of service via a crafted HTTP request.	Splunk Light - Version(s): <=6.6.0 Splunk Light - Version(s): <=6.4 - 6.4.6, 6.2 - 6.2.13, 6.3 - 6.3.9, 6.5 - 6.5.2	Published -Published - Oct 23, 2018 CVE- 2018-7432 CVSS - 7.5 Vendor's Advisor - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7432 https://www.splunk.com/view/SP-CAAAP5T
Mozilla Firefox <63 and Firefox ESR <60.3 Unspecified Memory Safety Bugs Could Allow Remote Code Execution - CVE-2018-12390	Mozilla Firefox before 63, and Firefox ESR before 60.3 are prone to multiple memory safety bugs that could possibly allow remote code execution.	Firefox Version(s): < 63 Release, 60.3 ESR, Enterprise Linux Server Version(s): <= 6, 7, EUS 7.5 Enterprise Linux Workstatio Version(s): <= 6, 7	Published - Oct 28, 2018 CVE- 2018-12390 CVSS - 8.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12390 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12390
Polycom VVX 500 and VVX 601 Remote Information Disclosure Vulnerability via SIP - CVE-2018-18566	The SIP service in Polycom VVX 500 and 601 devices 5.8.0.12848 and earlier allow remote attackers to obtain sensitive phone configuration information, such as phone name and number, by leveraging use with an on-premise installation with Skype for Business.	Version(s): <= 5.8.0.12848	Published -Published - Oct 26, 2018 CVE- 2018-18566 CVSS - 5.3 Vendor's Advisor - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-18566 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18566
Mozilla Firefox <63 Remote File Save Misdirection Vulnerability via SameSite Cookies - CVE-2018-12402	Mozilla Firefox before 63 is vulnerable to saving the wrong resources with the "Save Page As..." function, which uses SameSite cookie data from cross-origin requests.	Version(s): <63 release	Published - Oct 28, 2018 CVE- 2018-12402 CVSS - 4.3 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12402 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12402
EE 4GEE HH70 Routers Credentials Disclosure Vulnerability - CVE-2018-10532	EE 4GEE HH70 Routers running firmware HH70_E1_02.00_19 are prone to a credential disclosure vulnerability which enables an attacker to discover hard coded credentials and subsequently login to the router via SSH as the root user.	Version(s): <= HH70_E1_02.00_19	Published -Published - Oct 28, 2018 CVE- 2018-10532 CVSS - 8.4 Vendor's Advisor - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10532 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10532
[cisco-sa-20181024-webex-injection] Cisco Webex Meetings and Productivity Tools Local Unspecified Vulnerability - CVE-2018-15442	A vulnerability in the update service of Cisco Webex Meetings Desktop App before 33.6.0 for Windows and Webex Productivity Tools 32.6.0 and on, up to and not including 33.0.5, for Windows, could allow an authenticated, local attacker to execute arbitrary commands as a privileged user. The vulnerability is due to insufficient validation of user-supplied parameters. An attacker could exploit this vulnerability by invoking the update service command with a crafted argument. An exploit could allow the attacker to run arbitrary commands with SYSTEM user privileges. While the CVSS Attack Vector metric denotes the requirement for an attacker to have local access, administrators should be aware that in Active Directory deployments, the vulnerability could be exploited remotely by leveraging the operating system remote management tools.	WebEx Meetings Version(s): <33.6.0 WebEx Productivity Tools = 32.6.0-33.0.4	Published - Oct 28, 2018 CVE- 2018-15442 CVSS - 7.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15442 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-15442
Microsoft Word JavaScript Code Execution in Online Video Feature	Microsoft Word in Microsoft Office 2016 and earlier is prone to a JavaScript code execution vulnerability in the Online Video feature. The vulnerability has not been confirmed by the vendor as of yet.	Microsoft Word Desktop Apps & Office Business Apps Version(s): <= 2013 SP1 RT, 2016 x64, 2016 x86, 2010 SP2 x64, 2010 SP2 x86, 2013 SP1 x64, 2013 SP1 x86	Published -Published - Oct 26, 2018 SVB-92851 CVSS - 8.8 Vendor's Advisor - https://www.businesswire.com/news/home/20181025005616/en/Cymulate-Finds-Logical-Bug-Microsoft-Office-Suite https://blog.cymulate.com/abusing-microsoft-office-online-video
Veritas NetBackup Appliance <3.1.2 Remote Code Execution Vulnerability - CVE-2018-18652	A remote command execution vulnerability in Veritas NetBackup Appliance before 3.1.2 allows authenticated administrators to execute arbitrary commands as root. This issue was caused by insufficient filtering of user provided input.	Version(s): < 3.1.1	Published - Oct 25, 2018 CVE- 2018-18652 CVSS - 7.2 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18652 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-18652