| PRODUCT | DESCRIPTION | AFFECTED VERSIONS | OTHER INFORMATION |
|---|---|---|---|
| F5 BIG-IP 13.0.0-13.1.0.5, 12.0.0-12.1.3.3 DoS to Adjacent VCMP Guests - CVE-2018-5518 | On F5 BIG-IP 13.0.0 through 13.1.0.5 or 12.0.0 through 12.1.3.3 (on LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, GTM, Link Controller, PEM, WebAccelerator, or WebSafe), malicious root users with access to a VCMP guest can cause a disruption of service on adjacent VCMP guests running on the same host. Exploiting this vulnerability causes the vCMPd process on the adjacent VCMP guest to restart and produce a core file. This issue is only exploitable on a VCMP guest which is operating in "host-only" or "bridged" mode. VCMP guests which are "isolated" are not impacted by this issue and do not provide mechanism to exploit the vulnerability. Guests which are deployed in "Appliance Mode" may be impacted however the exploit is not possible from an Appliance Mode guest. To exploit this vulnerability root access on a guest system deployed as "host-only" or "bridged" mode is required. | Version(s): <= 13.1.0 - 13.1.0.5, 12.0.0 - 12.1.3.3 | Published - May 01, 2018<br>CVE-2018-5518<br>CVSS - 7.4<br>Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5518<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5518 |
| IBM Sterling Connect:Direct for OpenVMS Remote Unspecified Vulnerability | On F5 BIG-IP 13.1.0-13.1.0.5 (on LTM, AAM, AFM, APM, ASM, Link Controller, PEM, WebAccelerator, or WebSafe), maliciously crafted HTTP/2 request frames can lead to denial of service. There is data plane exposure for virtual servers when the HTTP2 profile is enabled. There is no control plane exposure to this issue. | Version(s): <= 3.4.01, 3.4.00, 3.6.0, 3.6.0.1, 3.5.00 | Published - May 01, 2018<br>CVE-2013-4035<br>CVSS - 9.8<br>Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4035<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4035 |
| F5 BIG-IP 13.1.0-13.1.0.5 Remote DoS via Crafted HTTP/2 Request Frames - CVE-2018-5514 | IBM Sterling Connect:Direct for OpenVMS 3.4.00, 3.4.01, 3.5.00, 3.6.0, and 3.6.0.1 allow remote attackers to have unspecified impact by leveraging failure to reject client requests for an unencrypted session when used as the server in a TCP/IP session and configured for SSL encryption with the client. IBM X-Force ID: 86138. | Version(s): <= 13.1.0 - 13.1.0.5 | Published - May 01, 2018<br>CVE-2018-5514<br>CVSS - 7.5<br>Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5514<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5514 |
| Linux Kernel Local Restrictions Bypass Vulnerability - CVE-2018-1108 | Linux Kernel is prone to a local restrictions bypass vulnerability due to a predictable random number generator weakness in the 'drivers/char/random.c' source file. This issue stems from the implementation of random seed data. A local attacker could exploit this issue early in the boot sequence, by using the data allocated for the seed before it was sufficiently generated to bypass certain security restrictions and perform unauthorized actions. | Version(s): <= 4.1.1 | Published - May 01, 2018<br>CVE-2018-1108<br>CVSS - 5.9<br>Vendor's Advisory - http://www.securityfocus.com/bid/104055<br>https://access.redhat.com/security/cve/cve-2018-1108 |
| LibreOffice and Apache OpenOffice Writer Remote Information Disclosure Vulnerability - CVE-2018-10583 | An information disclosure vulnerability occurs when LibreOffice 6.0.3 and Apache OpenOffice Writer 4.1.5 automatically process and initiate an SMB connection embedded in a malicious file, as demonstrated by xlink:href=file://192.168.0.2/test.jpg within an office:document-content element in a .odt XML document. | Version(s): <= Apache OpenOffice 4.1.5<br>LibreOffice 6.0.3 | Published - May 01, 2018<br>CVE-2018-10583<br>CVSS - 5.3<br>Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10583<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10583 |
| IBM Tivoli Application Dependency Discovery Manager on Unix Local Weak Permissions Vulnerability | IBM Tivoli Application Dependency Discovery Manager (TADDM) 7.1.2.x before 7.2.1.5 and 7.2.x before 7.2.1.5 on Unix use weak permissions (755) for unspecified configuration and log files, which allows local users to obtain sensitive information by reading the files. IBM X-Force ID: 86176. | Version(s): <= 7.1.2 - 7.2.1.4 | Published - May 01, 2018<br>CVE-2013-4040<br>CVSS - 4.0<br>Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4040<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4040 |
| [cisco-sa-20180502-war] Cisco WebEx Products Remote Code Execution Vulnerability via ARF File - CVE-2018-0264 | A vulnerability in the Cisco WebEx Network Recording Player for Advanced Recording Format (ARF) files could allow an unauthenticated, remote attacker to execute arbitrary code on the system of a targeted user. An attacker could exploit this vulnerability by sending the user a link or email attachment with a malicious ARF file and persuading the user to follow the link or open the file. Successful exploitation could allow the attacker to execute arbitrary code on the user's system. This vulnerability affects Cisco WebEx Business Suite meeting sites, Cisco WebEx Meetings sites, Cisco WebEx Meetings Server, and Cisco WebEx ARF players. The following client builds of Cisco WebEx Business Suite (WBS31 and WBS32), Cisco WebEx Meetings, and Cisco WebEx Meetings Server are affected: Cisco WebEx Business Suite (WBS31) client builds prior to T31.23.4, Cisco WebEx Business Suite (WBS32) client builds prior to T32.12, Cisco WebEx Meetings with client builds prior to T32.12, Cisco WebEx Meeting Server builds prior to 3.0 Patch 1. Cisco Bug IDs: CSCvh85410, CSCvh85430, CSCvh85440, CSCvh85442, CSCvh85453, CSCvh85457. | Version(s): < T32 - T32.11,T31.23.3 | Published - May 02, 2018<br>CVE-2018-0264<br>CVSS - 9.6<br>Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0264<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0264 |
| [cisco-sa-20180502-acs1] Cisco Secure Access Control System Remote Code Execution Vulnerability - CVE-2018-0253 | A vulnerability in the ACS Report component of Cisco Secure Access Control System (ACS) could allow an unauthenticated, remote attacker to execute arbitrary commands on an affected system. Commands executed by the attacker are processed at the targeted user's privilege level. The vulnerability is due to insufficient validation of the Action Message Format (AMF) protocol. An attacker could exploit this vulnerability by sending a crafted AMF message that contains malicious code to a targeted user. A successful exploit could allow the attacker to execute arbitrary commands on the ACS device. This vulnerability affects all releases of Cisco Secure ACS prior to Release 5.8 Patch 7. Cisco Bug IDs: CSCve69037. | Version(s): <=5.8 patch 9 | Published - May 02, 2018<br>CVE-2017-<br>CVE-2018-0253 -<br>Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0253<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0253 |
| Linux Kernel Remote DoS Vulnerability in Coresight/coresight-etm-perf.c - CVE-2018-11232 | Linux Kernel Remote DoS Vulnerability in Coresight/coresight-etm-perf.c - CVE-2018-11232<br>The etm_setup_aux function in drivers/hwtracing/coresight/coresight-etm-perf.c in the Linux kernel before 4.10.2 allows attackers to cause a denial of service (panic) because a parameter is incorrectly used as a local variable. | Version(s): <= 4.10.2 | Published - May 18, 2018<br>CVE-2018-11232<br>CVSS - 7.5<br>Vendor's Advisory - https://www.kernel.org/category/releases.html<br>http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11232 |
| Mozilla Thunderbird <52.8 Remote Information Disclosure Vulnerability due to Weak Encryption (EFAIL) - CVE-2018-5185 | Mozilla Thunderbird <52.8 Remote Information Disclosure Vulnerability due to Weak Encryption (EFAIL) - CVE-2018-5185<br>Mozilla Thunderbird before 52.8 is vulnerable to information disclosure in the form of plaintext email content being accessed through a malicious embedded HTML form submitted by a user. This is related to the "EFAIL" vulnerabilities. | Version(s): <= 52.8 | Published - May 18, 2018<br>CVE-2018-51858<br>CVSS - 7.5<br>Vendor's Advisory - https://www.thunderbird.net/en-US/<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5185 |
| CoreOS Tectonic Remote Information Disclosure Vulnerability in Kubernetes - CVE-2018-5256 | CoreOS Tectonic Remote Information Disclosure Vulnerability in Kubernetes - CVE-2018-5256<br>CoreOS Tectonic 1.7.x before 1.7.9-tectonic.4 and 1.8.x before 1.8.4-tectonic.3 mounts a direct proxy to the kubernetes cluster at /api/kubernetes/ which is accessible without authentication to Tectonic and allows an attacker to directly connect to the kubernetes API server. Unauthenticated users are able to list all Namespaces through the Console, resulting in an information disclosure. Tectonic's exposure of an unauthenticated API endpoint containing information regarding the internal state of the cluster can provide an attacker with information that may assist in other attacks against the cluster. For example, an attacker may not have the permissions required to list all namespaces in the cluster but can instead leverage this vulnerability to enumerate the namespaces and then begin to check each namespace for weak authorization policies that may allow further escalation of privileges. | Version(s): <= 1.8 - 1.8.4\- tecttonic.2, 1.7- 1..79 | Published - May 18, 2018<br>CVE-2018-5256<br>CVSS - 5.3<br>Vendor's Advisory - https://coreos.com/tectonic/docs/latest/admin/upgrade.html<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5185 |
| Linux Kernel Local Restriction Bypass or DoS Vulnerability via Keyrings - CVE-2017-18270 | Linux Kernel Local Restriction Bypass or DoS Vulnerability via Keyrings - CVE-2017-18270<br>In the Linux kernel before 4.13.5, a local user could create keyrings for other users via keyctl commands, setting unwanted defaults or causing a denial of service. | Version(s): <= 4.13.5 | Published - May 18, 2018<br>CVE-2018-18270<br>CVSS - 6.8<br>Vendor's Advisory - https://www.kernel.org/category/releases.html<br>http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18270 |
| Citrix NetScaler ADC and Gateway Remote Code Execution Vulnerability - CVE-2018-7218 | Citrix NetScaler ADC and Gateway Remote Code Execution Vulnerability - CVE-2018-7218<br>The AppFirewall functionality in Citrix NetScaler Application Delivery Controller and NetScaler Gateway 10.5 before Build 68.7, 11.0 before Build 71.24, 11.1 before Build 58.13, and 12.0 before Build 57.24 allows remote attackers to execute arbitrary code via unspecified vectors. | Version(s): <= 10.5-10.5. Biuld 57.13.0120. | Published - May 18, 2018<br>CVE-2018-7218<br>CVSS - 9.8<br>Vendor's Advisory - https://www.citrix.com/downloads/netscaler-adc.html<br>http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7218 |
| [cisco-sa-20180516-dna] Cisco DNA Center Remote Unauthorized Access Vulnerability - CVE-2018-0268 | [cisco-sa-20180516-dna] Cisco DNA Center Remote Unauthorized Access Vulnerability - CVE-2018-0268<br>A vulnerability in the container management subsystem of Cisco Digital Network Architecture (DNA) Center could allow an unauthenticated, remote attacker to bypass authentication and gain elevated privileges. This vulnerability is due to an insecure default configuration of the Kubernetes container management subsystem within DNA Center. An attacker who has the ability to access the Kubernetes service port could execute commands with elevated privileges within provisioned containers. A successful exploit could result in a complete compromise of affected containers. This vulnerability affects Cisco DNA Center Software Releases 1.1.3 and prior. Cisco Bug IDs: CSCvi47253. | Version(s): <= 1.1.3 | Published - May 18, 2018<br>CVE-2018-0268<br>CVSS - 10.0<br>Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0268<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0268<br>http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-dna |

| PRODUCT | DESCRIPTION | AFFECTED VERSIONS | OTHER INFORMATION |
|---|---|---|---|
| [cisco-sa-20180516-dna2] Cisco DNA Center Remote Authentication Bypass Vulnerability - CVE-2018-0271 | [cisco-sa-20180516-dna2] Cisco DNA Center Remote Authentication Bypass Vulnerability - CVE-2018-0271<br>A vulnerability in the API gateway of the Cisco Digital Network Architecture (DNA) Center could allow an unauthenticated, remote attacker to bypass authentication and access critical services. The vulnerability is due to a failure to normalize URLs prior to servicing requests. An attacker could exploit this vulnerability by submitting a crafted URL designed to exploit the issue. A successful exploit could allow the attacker to gain unauthenticated access to critical services, resulting in elevated privileges in DNA Center. This vulnerability affects Cisco DNA Center Software Releases prior to 1.1.2. Cisco Bug IDs: CSCvi09394 | Version(s): <= .1.1.2 | Published - May 01, 2018<br>CVE-2018-<br>CVSS -<br>Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0271<br>http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0271 |