# National Critical Information Infrastructure Protection Centre

## *CVE Report*

**01-15 February 2017** **Vol. 04 No. 03**

| Vulnerability Type(s) | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Application (A)** | | | | | |
| **Adobe** | | | | | |
| ***Campaign***<br>Adobe Campaign, part of Adobe Marketing Cloud, helps you achieve your cross-channel marketing goals. | | | | | |
| Cross Site Scripting | 15-02-2017 | 4.3 | Adobe Campaign versions 16.4 Build 8724 and earlier have a cross-site scripting (XSS) vulnerability.<br>**REFERENCE: CVE-2017-2969** | https://helpx.adobe.com/security/products/campaign/apsb17-03.html | A-ADO-CAMPA-280217/01 |
| NA | 15-02-2017 | 7.5 | Adobe Campaign versions 16.4 Build 8724 and earlier have a code injection vulnerability.<br>**REFERENCE: CVE-2017-2968** | https://helpx.adobe.com/security/products/campaign/apsb17-03.html | A-ADO-CAMPA-280217/02 |
| ***Digital Editions***<br>Adobe Digital Editions (abbreviated ADE) is an ebook reader software program from Adobe Systems, built initially (1.x version) using Adobe Flash. | | | | | |
| Execute Code; Overflow; Memory Corruption | 15-02-2017 | 5 | Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.<br>**REFERENCE: CVE-2017-2981** | https://helpx.adobe.com/security/products/Digital-Editions/apsb17-05.html | A-ADO-DIGIT-280217/03 |
| Execute Code; Overflow; Memory Corruption | 15-02-2017 | 5 | Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.<br>**REFERENCE: CVE-2017-2980** | https://helpx.adobe.com/security/products/Digital-Editions/apsb17-05.html | A-ADO-DIGIT-280217/04 |
| Execute Code; | 15-02-2017 | 5 | Adobe Digital Editions | https://helpx.a | A-ADO- |

| | | | | | |
|---|---|---|---|---|---|
| Overflow; Memory Corruption | | | versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2017-2979** | dobe.com/security/products/Digital-Editions/apsb17-05.html | DIGIT-280217/05 |
| Execute Code; Overflow; Memory Corruption | 15-02-2017 | 5 | Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2017-2978** | https://helpx.adobe.com/security/products/Digital-Editions/apsb17-05.html | A-ADO-DIGIT-280217/06 |
| Execute Code; Overflow; Memory Corruption | 15-02-2017 | 5 | Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2017-2977** | https://helpx.adobe.com/security/products/Digital-Editions/apsb17-05.html | A-ADO-DIGIT-280217/07 |
| Execute Code; Overflow; Memory Corruption | 15-02-2017 | 5 | Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2017-2976** | https://helpx.adobe.com/security/products/Digital-Editions/apsb17-05.html | A-ADO-DIGIT-280217/08 |
| Execute Code; Overflow; Memory Corruption | 15-02-2017 | 5 | Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2017-2975** | https://helpx.adobe.com/security/products/Digital-Editions/apsb17-05.html | A-ADO-DIGIT-280217/09 |
| Execute Code; | 15-02-2017 | 5 | Adobe Digital Editions | https://helpx.a | A-ADO- |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Overflow; Memory Corruption | | | versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2017-2974** | dobe.com/security/products/Digital-Editions/apsb17-05.html | DIGIT-280217/10 |
| Execute Code; Overflow | 15-02-2017 | 10 | Adobe Digital Editions versions 4.5.3 and earlier have an exploitable heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2017-2973** | https://helpx.adobe.com/security/products/Digital-Editions/apsb17-05.html | A-ADO-DIGIT-280217/11 |
| ***Flash Player***<br>Adobe Flash Player is freeware software for using content created on the Adobe Flash platform, including viewing multimedia, executing rich Internet applications, and streaming video and audio. | | | | | |
| Execute Code | 15-02-2017 | 6.8 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable type confusion vulnerability related to the MessageChannel class. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2017-2995** | https://helpx.adobe.com/security/products/flash-player/apsb17-04.html | A-ADO-FLASH-280217/12 |
| Execute Code | 15-02-2017 | 6.8 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in Primetime SDK event dispatch. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2017-2994** | https://helpx.adobe.com/security/products/flash-player/apsb17-04.html | A-ADO-FLASH-280217/13 |
| Execute Code; Overflow; Memory Corruption | 15-02-2017 | 10 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption | https://helpx.adobe.com/security/products/flash- | A-ADO-FLASH-280217/14 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | vulnerability in Primetime SDK. Successful exploitation could lead to arbitrary code execution.<br>**REFERENCE: CVE-2017-2996** | player/apsb17-04.html | |
| Execute Code | 15-02-2017 | 10 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability related to event handlers. Successful exploitation could lead to arbitrary code execution.<br>**REFERENCE: CVE-2017-2993** | https://helpx.adobe.com/security/products/flash-player/apsb17-04.html | A-ADO-FLASH-280217/15 |
| Execute Code; Overflow | 15-02-2017 | 10 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability when parsing an MP4 header. Successful exploitation could lead to arbitrary code execution.<br>**REFERENCE: CVE-2017-2992** | https://helpx.adobe.com/security/products/flash-player/apsb17-04.html | A-ADO-FLASH-280217/16 |
| Execute Code; Overflow; Memory Corruption | 15-02-2017 | 10 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability in the h264 codec (related to decompression). Successful exploitation could lead to arbitrary code execution.<br>**REFERENCE: CVE-2017-2991** | https://helpx.adobe.com/security/products/flash-player/apsb17-04.html | A-ADO-FLASH-280217/17 |
| Execute Code; Overflow; Memory Corruption | 15-02-2017 | 10 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability in the h264 decompression routine. Successful exploitation could lead to arbitrary code | https://helpx.adobe.com/security/products/flash-player/apsb17-04.html | A-ADO-FLASH-280217/18 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | execution.<br>**REFERENCE: CVE-2017-2990** | | |
| Execute Code; Overflow; Memory Corruption | 15-02-2017 | 10 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability when performing garbage collection. Successful exploitation could lead to arbitrary code execution.<br>**REFERENCE: CVE-2017-2988** | https://helpx.adobe.com/security/products/flash-player/apsb17-04.html | A-ADO-FLASH-280217/19 |
| Execute Code; Overflow | 15-02-2017 | 10 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable integer overflow vulnerability related to Flash Broker COM. Successful exploitation could lead to arbitrary code execution.<br>**REFERENCE: CVE-2017-2987** | https://helpx.adobe.com/security/products/flash-player/apsb17-04.html | A-ADO-FLASH-280217/20 |
| Execute Code; Overflow | 15-02-2017 | 10 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability in the Flash Video (FLV) codec. Successful exploitation could lead to arbitrary code execution.<br>**REFERENCE: CVE-2017-2986** | https://helpx.adobe.com/security/products/flash-player/apsb17-04.html | A-ADO-FLASH-280217/21 |
| Execute Code | 15-02-2017 | 10 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in the ActionScript 3 BitmapData class. Successful exploitation could lead to arbitrary code execution.<br>**REFERENCE: CVE-2017-** | https://helpx.adobe.com/security/products/flash-player/apsb17-04.html | A-ADO-FLASH-280217/22 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | **2985** | | |
| Execute Code; Overflow | 15-02-2017 | 10 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability in the h264 decoder routine. Successful exploitation could lead to arbitrary code execution.<br>**REFERENCE: CVE-2017-2984** | https://helpx.adobe.com/security/products/flash-player/apsb17-04.html | A-ADO-FLASH-280217/23 |
| Execute Code | 15-02-2017 | 10 | Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in a routine related to player shutdown. Successful exploitation could lead to arbitrary code execution.<br>**REFERENCE: CVE-2017-2982** | https://helpx.adobe.com/security/products/flash-player/apsb17-04.html | A-ADO-FLASH-280217/24 |
| **Advantech** | | | | | |
| ***Susiaccess***<br>Advantech has made a big push, and is now unveiling the latest version of SUSIAccess 3.0, aiming to accelerate the adoption of device designs and ensuring manageability, security, and connectivity. | | | | | |
| Gain Information | 13-02-2017 | 5 | An issue was discovered in Advantech SUISAccess Server Version 3.0 and prior. An attacker could traverse the file system and extract files that can result in information disclosure.<br>**REFERENCE: CVE-2016-9349** | NA | A-ADV-SUSIA-280217/25 |
| Directory Traversal | 13-02-2017 | 6 | An issue was discovered in Advantech SUISAccess Server Version 3.0 and prior. The directory traversal/file upload error allows an attacker to upload and unpack a zip file.<br>**REFERENCE: CVE-2016-9351** | NA | A-ADV-SUSIA-280217/26 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| NA | 13-02-2017 | 7.2 | An issue was discovered in Advantech SUISAccess Server Version 3.0 and prior. The admin password is stored in the system and is encrypted with a static key hard-coded in the program. Attackers could reverse the admin account password for use.<br>**REFERENCE: CVE-2016-9353** | NA | A-ADV-SUSIA-280217/27 |
| ***Webaccess***<br>Advantech WebAccess is a web browser-based software package for HMI/SCADA software. | | | | | |
| Bypass | 13-02-2017 | 6.4 | An issue was discovered in Advantech WebAccess Version 8.1. By accessing a specific uniform resource locator (URL) on the web server, a malicious user is able to access pages unrestricted (AUTHENTICATION BYPASS).<br>**REFERENCE: CVE-2017-5152** | NA | A-ADV-WEBAC-280217/28 |
| SQL Injection | 13-02-2017 | 7.5 | An issue was discovered in Advantech WebAccess Version 8.1. To be able to exploit the SQL injection vulnerability, an attacker must supply malformed input to the WebAccess software. Successful attack could result in administrative access to the application and its data files.<br>**REFERENCE: CVE-2017-5154** | NA | A-ADV-WEBAC-280217/29 |
| **Artifex** | | | | | |
| ***Mupdf***<br>MuPDF is a free and open-source software framework written in C that implements a PDF, XPS, and EPUB parsing and rendering engine. | | | | | |
| Denial of | 15-02-2017 | 4.3 | Heap-based buffer | https://bugs.gh | A-ART- |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Service; Overflow | | | overflow in the fz_subsample_pixmap function in fitz/pixmap.c in MuPDF 1.10a allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted image.<br>**REFERENCE: CVE-2017-5896** | ostscript.com/show_bug.cgi?id=697515 | MUPDF-280217/30 |
| Denial of Service | 15-02-2017 | 4.3 | The pdf_to_num function in pdf-object.c in MuPDF before 1.10 allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted file.<br>**REFERENCE: CVE-2016-8674** | https://bugzilla.redhat.com/show_bug.cgi?id=1385685 | A-ART-MUPDF-280217/31 |
| NA | 15-02-2017 | 5 | An issue was discovered in Artifex Software, Inc. MuPDF before 1912de5f08e90af1d9d0a9791f58ba3afdb9d465. The pdf_run_xobject function in pdf-op-run.c encounters a NULL pointer dereference during a Fitz fz_paint_pixmap_with_mask painting operation.<br>**REFERENCE: CVE-2017-5991** | https://bugs.ghostscript.com/show_bug.cgi?id=697500 | A-ART-MUPDF-280217/32 |
| **Atutor** | | | | | |
| ***Atutor***<br>ATutor is a free Open Source Learning Management System designed with accessibility and adaptability in mind. | | | | | |
| Execute Code; Cross Site Request Forgery | 07-02-2017 | 6.8 | Cross-site request forgery (CSRF) vulnerability in install_modules.php in ATutor before 2.2.2 allows remote attackers to hijack the authentication of users for requests that upload arbitrary files and execute arbitrary PHP code via | https://github.com/atutor/ATutor/commit/bfc6c80c6c217c5515172f3cc949e13dfa1a92ac | A-ATU-ATUTO-280217/33 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | vectors involving a crafted zip file.<br>**REFERENCE: CVE-2016-2539** | | |
| **Autotrace Project** | | | | | |
| ***Autotrace***<br>Autotrace is a program which converts bitmap images to vector images. | | | | | |
| Denial of Service; Overflow | 15-02-2017 | 4.3 | Heap-based buffer overflow in the pstoedit_suffix_table_init function in output-pstoedit.c in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted bmp image file.<br>**REFERENCE: CVE-2016-7392** | https://bugzilla.redhat.com/show_bug.cgi?id=1375255 | A-AUT-AUTOT-280217/34 |
| **Bigtreecms** | | | | | |
| ***Bigtree Cms***<br>BigTree CMS is an open source content management system built on PHP and MySQL. | | | | | |
| Execute Code | 14-02-2017 | 3.5 | An issue was discovered in BigTree CMS before 4.2.15. The vulnerability exists due to insufficient filtration of user-supplied data in the "id" HTTP GET parameter passed to the "core/admin/adjax/dashboard/check-module-integrity.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.<br>**REFERENCE: CVE-2016-10223** | https://github.com/bigtreecms/BigTree-CMS/blob/master/README.md | A-BIG-BIGTR-280217/35 |
| **Bubblewrap Project** | | | | | |
| ***Bubblewrap***<br>Bubble Wrap is a program developed by XM Asia Pacific Pte Ltd. The main program executable isBubbleWrap.exe. | | | | | |
| Gain Privileges | 13-02-2017 | 6.9 | Bubblewrap before 0.1.3 sets the | https://github.com/projectato | A-BUB-BUBBL- |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | PR_SET_DUMPABLE flag, which might allow local users to gain privileges by attaching to the process, as demonstrated by sending commands to a PrivSep socket.<br>**REFERENCE: CVE-2016-8659** | mic/bubblewrap/issues/107 | 280217/36 |
| **Busybox** | | | | | |
| ***Busybox***<br>BusyBox is a software that provides several stripped-down Unix tools in a single executable file. | | | | | |
| Denial of Service; Overflow | 09-02-2017 | 5 | Integer overflow in the DHCP client (udhcpc) in BusyBox before 1.25.0 allows remote attackers to cause a denial of service (crash) via a malformed RFC1035-encoded domain name, which triggers an out-of-bounds heap write.<br>**REFERENCE: CVE-2016-2147** | https://git.busybox.net/busybox/commit/?id=d474ffc68290e0a83651c4432eeabfa62cd51e87 | A-BUS-BUSYB-280217/37 |
| Overflow | 09-02-2017 | 7.5 | Heap-based buffer overflow in the DHCP client (udhcpc) in BusyBox before 1.25.0 allows remote attackers to have unspecified impact via vectors involving OPTION_6RD parsing.<br>**REFERENCE: CVE-2016-2148** | https://busybox.net/news.html | A-BUS-BUSYB-280217/38 |
| **Cairographics** | | | | | |
| ***Cairo***<br>Cairo is a 2D graphics library with support for multiple output devices. | | | | | |
| Denial of Service; Overflow | 03-02-2017 | 4.3 | Integer overflow in the write_png function in cairo 1.14.6 allows remote attackers to cause a denial of service (invalid pointer dereference) via a large svg file.<br>**REFERENCE: CVE-2016-9082** | https://bugs.freedesktop.org/attachment.cgi?id=127421 | A-CAI-CAIRO-280217/39 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| **Chatsecure;ZOM** |  |  |  |  |  |
| ***Chatsecure/ZOM***<br>ChatSecure is a free and open source messaging app that features OTR encryption over XMPP/ Zom is the next generation communication app based on ChatSecure focused on hyper usability. |  |  |  |  |  |
| NA | 09-02-2017 | 4.3 | An incorrect implementation of "XEP-0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This CVE is for ChatSecure (3.2.0 - 4.0.0; only iOS) and Zom (all versions up to 1.0.11; only iOS).<br>**REFERENCE: CVE-2017-5590** | NA | A-CHA-CHATS-280217/40 |
| **Cisco** |  |  |  |  |  |
| ***Activetouch General Plugin Container; Download Manager; Gpccontainer Class; Webex; Webex Meeting Center; Webex Meetings Server***<br>Cisco WebEx, formerly WebEx Communications Inc. is a company that provides on-demand collaboration, online meeting, web conferencing and videoconferencing applications; Cisco WebEx Meeting Center provides cost-effective enterprise video conferencing; Cisco WebEx Meetings Server is a cost-effective, secure, and flexible collaboration and communications solution for your private cloud; NA |  |  |  |  |  |
| Execute Code; Overflow | 01-02-2017 | 9.3 | An issue was discovered in the Cisco WebEx Extension before 1.0.7 on Google Chrome, the ActiveTouch General Plugin Container before 106 on Mozilla Firefox, the GpcContainer Class ActiveX control plugin before 10031.6.2017.0126 on Internet Explorer, and the Download Manager ActiveX control plugin before 2.1.0.10 on Internet Explorer. Vulnerability in these Cisco WebEx browser | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170124-webex | A-CIS-ACTIV-280217/41 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server and Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) when they are running on Microsoft Windows. The vulnerability is a design defect in an application programing interface (API) response parser within the extension. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser.<br>**REFERENCE: CVE-2017-3823** | | |
| ***Anyconnect Secure Mobility Client***<br>Cisco's AnyConnect VPN is a Virtual Private Network (VPN) client. | | | | | |
| Execute Code | 09-02-2017 | 7.2 | Vulnerability in the Start Before Logon (SBL) module of Cisco AnyConnect Secure Mobility Client Software for Windows could allow an unauthenticated, local attacker to open Internet Explorer with the privileges of the SYSTEM | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170208-anyconnect | A-CIS-ANYCO-280217/42 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | user. The vulnerability is due to insufficient implementation of the access controls. An attacker could exploit this vulnerability by opening the Internet Explorer browser. An exploit could allow the attacker to use Internet Explorer with the privileges of the SYSTEM user. This may allow the attacker to execute privileged commands on the targeted system. This vulnerability affects versions prior to released versions 4.4.00243 and later and 4.3.05017 and later. Cisco Bug IDs: CSCvc43976.<br>**REFERENCE: CVE-2017-3813** |  |  |
| ***Cisco Prime Home***<br>Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, reduces operational costs and improves the subscriber experience. |  |  |  |  |  |
| Execute Code; Bypass | 01-02-2017 | 10 | Vulnerability in the web-based GUI of Cisco Prime Home could allow an unauthenticated, remote attacker to bypass authentication and execute actions with administrator privileges. The vulnerability is due to a processing error in the role-based access control (RBAC) of URLs. An attacker could exploit this vulnerability by sending API commands via HTTP to a particular URL without prior authentication. An exploit could allow the | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-prime-home | A-CIS-CISCO-280217/43 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | attacker to perform any actions in Cisco Prime Home with administrator privileges. This vulnerability affects Cisco Prime Home versions from 6.3.0.0 to the first fixed release 6.5.0.1. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. Cisco Bug IDs: CSCvb49837.<br>**REFERENCE: CVE-2017-3791** | | |
| ***Firepower Management Center***<br>The Cisco Firepower Management Center (formerly FireSIGHT Management Center) is the administrative nerve center for select Cisco security products running on a number of different platforms. | | | | | |
| Bypass | 03-02-2017 | 5 | Vulnerability in Cisco Firepower System Software could allow an unauthenticated, remote attacker to maliciously bypass the appliance's ability to block certain web content, aka a URL Bypass. More Information: CSCvb93980. Known Affected Releases: 5.3.0 5.4.0 6.0.0 6.0.1 6.1.0.<br>**REFERENCE: CVE-2017-3814** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-fpw1 | A-CIS-FIREP-280217/44 |
| NA | 03-02-2017 | 5 | Vulnerability in the Policy deployment module of the Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to prevent deployment of a complete and accurate rule base. More Information: CSCvb95281. Known | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-fmc | A-CIS-FIREP-280217/45 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | Affected Releases: 6.1.0 6.2.0. Known Fixed Releases: 6.1.0.1 6.2.0. **REFERENCE: CVE-2017-3809** | | |
| ***Prime Service Catalog***<br>Cisco Prime Service Catalog provides a self-service portal, service-request management, and an IT service catalog for data center to desktop services. | | | | | |
| NA | 03-02-2017 | 4.9 | Vulnerability in the web framework of Cisco Prime Service Catalog could allow an authenticated, remote attacker to conduct a web URL redirect attack against a user who is logged in to an affected system. More Information: CSCvb21745. Known Affected Releases: 10.0_R2_tanggula. **REFERENCE: CVE-2017-3810** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-psc | A-CIS-PRIME-280217/46 |
| ***Telepresence Mcu Software***<br>The Cisco TelePresence MCU 5300 Series is a range of state-of-the-art multipoint control units (MCUs) that can grow with your video usage over the long term. | | | | | |
| Denial of Service; Execute Code; Overflow | 01-02-2017 | 10 | Vulnerability in a proprietary device driver in the kernel of Cisco TelePresence Multipoint Control Unit (MCU) Software could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. The vulnerability is due to improper size validation when reassembling fragmented IPv4 or IPv6 packets. An attacker could exploit this vulnerability by sending crafted IPv4 or IPv6 fragments to a port receiving content in Passthrough content mode. | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170125-telepresence | A-CIS-TELEP-280217/47 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | An exploit could allow the attacker to overflow a buffer. If successful, the attacker could execute arbitrary code or cause a DoS condition on the affected system. Cisco TelePresence MCU platforms TelePresence MCU 5300 Series, TelePresence MCU MSE 8510 and TelePresence MCU 4500 are affected when running software version 4.3(1.68) or later configured for Passthrough content mode. Cisco has released software updates that address this vulnerability. Workarounds that address this vulnerability are not available, but mitigations are available. Cisco Bug IDs: CSCuu67675. **REFERENCE: CVE-2017-3792** | | |
| ***Unified Computing System Director***<br>Cisco UCS Director is a unified infrastructure management solution that makes it easier to manage Vblock, FlexPod, and VSPEX environments. | | | | | |
| NA | 15-02-2017 | 4.6 | Vulnerability in the web-based GUI of Cisco UCS Director 6.0.0.0 and 6.0.0.1 could allow an authenticated, local attacker to execute arbitrary workflow items with just an end-user profile, a Privilege Escalation Vulnerability. The vulnerability is due to improper role-based access control (RBAC) after the Developer Menu is enabled in Cisco UCS Director. An | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-ucs | A-CIS-UNIFI-280217/48 |

| CV Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | attacker could exploit this vulnerability by enabling Developer Mode for his/her user profile with an end-user profile and then adding new catalogs with arbitrary workflow items to his/her profile. An exploit could allow an attacker to perform any actions defined by these workflow items, including actions affecting other tenants. Cisco Bug IDs: CSCvb64765.<br>**REFERENCE: CVE-2017-3801** | | |
| **Conversejs** | | | | | |
| ***Converse.js***<br>Converse.js is a free and open-source XMPP chat client in your browser. | | | | | |
| NA | 09-02-2017 | 4.3 | An incorrect implementation of "XEP-0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This CVE is for Converse.js (0.8.0 - 1.0.6, 2.0.0 - 2.0.4).<br>**REFERENCE: CVE-2017-5858** | NA | A-CON-CONVE-280217/49 |
| **Dhcpcd Project** | | | | | |
| ***Dhcpcd***<br>dhcpcd is an implementation of the DHCP client specified in RFC2131 (when -r option is not specified) and RFC1541 (when -r option is specified). | | | | | |
| Denial of Service; Overflow | 07-02-2017 | 5 | dhcpcd before 6.10.0 allows remote attackers to cause a denial of service (invalid read and crash) via vectors related to the option length. | http://roy.marples.name/projects/dhcpcd/info/595883e2a431f65d8fabf33059aa4689cca174 | A-DHC-DHCPC-280217/50 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | **REFERENCE: CVE-2016-1504** | 03 |  |
| **Dotclear** |  |  |  |  |  |
| ***Dotclear***<br>Dotclear is an open source blog publishing application distributed under the GNU GPLv2. |  |  |  |  |  |
| Cross Site Scripting | 09-02-2017 | 4.3 | Cross-site scripting (XSS) vulnerability in admin/comments.php in Dotclear before 2.8.2 allows remote attackers to inject arbitrary web script or HTML via the author name in a comment. **REFERENCE: CVE-2015-8831** | https://hg.dotclear.org/dotclear/rev/65e65154dadf | A-DOT-DOTCL-280217/51 |
| Execute Code | 09-02-2017 | 6.5 | Multiple incomplete blacklist vulnerabilities in inc/core/class.dc.core.php in Dotclear before 2.8.2 allow remote authenticated users with "manage their own media items" and "manage their own entries and comments" permissions to execute arbitrary PHP code by uploading a file with a (1) .pht, (2) .phps, or (3) .phtml extension. **REFERENCE: CVE-2015-8832** | https://hg.dotclear.org/dotclear/rev/198580bc3d80 | A-DOT-DOTCL-280217/52 |
| **Dotcms** |  |  |  |  |  |
| ***Dotcms***<br>dotCMS is a open source content management system and headless CMS for managing and delivering content driven web apps and sites. |  |  |  |  |  |
| Cross Site Scripting | 06-02-2017 | 3.5 | XSS was discovered in dotCMS 3.7.0, with an authenticated attack against the /myAccount addressID parameter. **REFERENCE: CVE-2017-5875** | NA | A-DOT-DOTCM-280217/53 |
| Cross Site Scripting | 06-02-2017 | 4.3 | XSS was discovered in dotCMS 3.7.0, with an unauthenticated attack | NA | A-DOT-DOTCM-280217/54 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | against the /about-us/locations/index direction parameter.<br>**REFERENCE: CVE-2017-5877** | | |
| Cross Site Scripting | 06-02-2017 | 4.3 | XSS was discovered in dotCMS 3.7.0, with an unauthenticated attack against the /news-events/events date parameter.<br>**REFERENCE: CVE-2017-5876** | NA | A-DOT-DOTCM-280217/55 |
| **Dotnetnuke** | | | | | |
| ***Dotnetnuke***<br>DNN (formerly DotNetNuke) is a web content management system based on Microsoft .NET. | | | | | |
| NA | 06-02-2017 | 7.5 | The installation wizard in DotNetNuke (DNN) before 7.4.1 allows remote attackers to reinstall the application and gain SuperUser access via a direct request to Install/InstallWizard.aspx.<br>**REFERENCE: CVE-2015-2794** | http://www.dnnsoftware.com/community-blog/cid/155198/workaround-for-potential-security-issue | A-DOT-DOTNE-280217/56 |
| **EMC** | | | | | |
| ***Isilon Insightiq***<br>EMC Isilon data management software provides you with powerful tools to optimize storage resources and system performance. | | | | | |
| Bypass | 08-02-2017 | 7.5 | EMC Isilon InsightIQ 4.1.0, 4.0.1, 4.0.0, 3.2.2, 3.2.1, 3.2.0, 3.1.1, 3.1.0, 3.0.1, 3.0.0 is affected by an authentication bypass vulnerability that could potentially be exploited by attackers to compromise the affected system.<br>**REFERENCE: CVE-2017-2765** | http://www.securityfocus.com/archive/1/540100/30/0/threaded | A-EMC-ISILO-280217/57 |
| **Exponentcms** | | | | | |
| ***Exponent Cms***<br>Exponent CMS is an Open Source Content Management System, based on PHP, MySQL and the Exponent Framework. | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| SQL Injection | 06-02-2017 | 7.5 | An issue was discovered in Exponent CMS 2.4.1. This is a blind SQL injection that can be exploited by un-authenticated users via an HTTP GET request and which can be used to dump database data out to a malicious server, using an out-of-band technique, such as select_loadfile(). The vulnerability affects source_selector.php and the following parameter: src.<br>**REFERENCE: CVE-2017-5879** | NA | A-EXP-EXPON-280217/58 |
| Execute Code; SQL Injection | 07-02-2017 | 7.5 | Multiple SQL injection vulnerabilities in Exponent CMS before 2.4.0 allow remote attackers to execute arbitrary SQL commands via the (1) id parameter in an activate_address address controller action, (2) title parameter in a show blog controller action, or (3) content_id parameter in a showComments expComment controller action.<br>**REFERENCE: CVE-2016-7400** | https://github.com/exponentcms/exponent-cms/commit/e916702a91a6342bbab483a2be2ba2f11dca3aa3 | A-EXP-EXPON-280217/59 |
| Execute Code | 13-02-2017 | 7.5 | install/index.php in Exponent CMS 2.3.9 allows remote attackers to execute arbitrary commands via shell metacharacters in the sc array parameter.<br>**REFERENCE: CVE-2016-7565** | https://exponentcms.lighthouseapp.com/projects/61783/changesets/4ae457ff1bf80e8b61286cd125ca794b25564e86 | A-EXP-EXPON-280217/60 |
| **Fatek** | | | | | |
| ***Automation Fv Designer; Automation Pm Designer***<br>Fv Designer is a software tool used to design and develop FATEK FV HMI series product projects; PM | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Designer is the program used to edit the settings of Fatek HMI hardware. | | | | | |
| Overflow | 13-02-2017 | 5 | An issue was discovered in Fatek Automation PM Designer V3 Version 2.1.2.2, and Automation FV Designer Version 1.2.8.0. By sending additional valid packets, an attacker could trigger a stack-based buffer overflow and cause a crash. Also, a malicious attacker can trigger a remote buffer overflow on the Fatek Communication Server.<br>**REFERENCE: CVE-2016-5798** | NA | A-FAT-AUTOM-280217/61 |
| Execute Code; Overflow | 13-02-2017 | 6.8 | An issue was discovered in Fatek Automation PM Designer V3 Version 2.1.2.2, and Automation FV Designer Version 1.2.8.0. Sending additional valid packets could allow the attacker to cause a crash or to execute arbitrary code, because of Improper Restriction of Operations within the Bounds of a Memory Buffer.<br>**REFERENCE: CVE-2016-5796** | NA | A-FAT-AUTOM-280217/62 |
| **Ffmpeg** | | | | | |
| ***Ffmpeg***<br>FFmpeg is a free software project that produces libraries and programs for handling multimedia data. | | | | | |
| Execute Code; Overflow | 09-02-2017 | 7.5 | Heap-based buffer overflow in ffserver.c in FFmpeg before 2.8.10, 3.0.x before 3.0.5, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 allows remote attackers to execute arbitrary code by leveraging failure to check chunk size.<br>**REFERENCE: CVE-2016-10192** | https://ffmpeg.org/security.html | A-FFM-FFMPE-280217/63 |

| CV Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Execute Code; Overflow | 09-02-2017 | 7.5 | Heap-based buffer overflow in libavformat/rtmppkt.c in FFmpeg before 2.8.10, 3.0.x before 3.0.5, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 allows remote attackers to execute arbitrary code by leveraging failure to check for RTMP packet size mismatches.<br>**REFERENCE: CVE-2016-10191** | https://ffmpeg.org/security.html | A-FFM-FFMPE-280217/64 |
| Execute Code; Overflow | 09-02-2017 | 7.5 | Heap-based buffer overflow in libavformat/http.c in FFmpeg before 2.8.10, 3.0.x before 3.0.5, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 allows remote web servers to execute arbitrary code via a negative chunk size in an HTTP response.<br>**REFERENCE: CVE-2016-10190** | https://trac.ffmpeg.org/ticket/5992 | A-FFM-FFMPE-280217/65 |
| **Froxlor** | | | | | |
| ***Froxlor***<br>froxlor Server Management Panel is the lightweight server management software for your needs. | | | | | |
| NA | 13-02-2017 | 5 | Froxlor before 0.9.35 uses the PHP rand function for random number generation, which makes it easier for remote attackers to guess the password reset token by predicting a value.<br>**REFERENCE: CVE-2016-5100** | https://github.com/Froxlor/Froxlor/commit/da4ec3e1b591de96675817a009e26e05e848a6ba | A-FRO-FROXL-280217/66 |
| **Gnome** | | | | | |
| ***Librsvg***<br>librsvg is a free software SVG rendering library written as part of the GNOME project, intended to be lightweight and portable. | | | | | |
| Denial of Service | 03-02-2017 | 4.3 | The rsvg_pattern_fix_fallback function in rsvg- | https://bugzilla.redhat.com/show_bug.cgi?id= | A-GNO-LIBRS-280217/67 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | paint_server.c in librsvg2 2.40.2 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted svg file.<br>**REFERENCE: CVE-2016-6163** | 1353520 | |
| **GNU** | | | | | |
| ***Libiberty***<br>The libiberty library is a collection of subroutines used by various GNU programs. | | | | | |
| Denial of Service; Overflow | 07-02-2017 | 5 | The demangler in GNU Libiberty allows remote attackers to cause a denial of service (infinite loop, stack overflow, and crash) via a cycle in the references of remembered mangled types.<br>**REFERENCE: CVE-2016-6131** | https://gcc.gnu.org/bugzilla/show_bug.cgi?id=71696 | A-GNU-LIBIB-280217/68 |
| **Gosa Project** | | | | | |
| ***Gosa Plugin***<br>GOsa is a combination of system-administrator and end-user web interface, designed to handle LDAP based setups. | | | | | |
| Cross Site Scripting | 13-02-2017 | 4.3 | Cross-site scripting (XSS) vulnerability in the displayLogin function in html/index.php in GOsa allows remote attackers to inject arbitrary web script or HTML via the username.<br>**REFERENCE: CVE-2014-9760** | https://github.com/gosa-project/gosa-core/commit/e35b990464a2c2cf64d6833a217ed944876e7732 | A-GOS-GOSA-280217/69 |
| **Gradle** | | | | | |
| ***Gradle***<br>Gradle is the next evolutionary step in JVM-based build tools. | | | | | |
| Execute Code | 07-02-2017 | 7.5 | ObjectSocketWrapper.java in Gradle 2.12 allows remote attackers to execute arbitrary code via a crafted serialized object.<br>**REFERENCE: CVE-2016-6199** | NA | A-GRA-GRADL-280217/70 |
| **Gstreamer Project** | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

***Gstreamer***

GStreamer is a pipeline-based multimedia framework that links together a wide variety of media processing systems to complete complex workflows.

| | | | | | |
|---|---|---|---|---|---|
| Denial of Service | 09-02-2017 | 4.3 | The gst_asf_demux_process_ext_stream_props function in gst/asfdemux/gstasfdemux.c in gst-plugins-ugly in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (invalid memory read and crash) via vectors related to the number of languages in a video file.<br>**REFERENCE: CVE-2017-5846** | https://gstreamer.freedesktop.org/releases/1.10/#1.10.3 | A-GST-GSTRE-280217/71 |
| Denial of Service | 09-02-2017 | 4.3 | The gst_riff_create_audio_caps function in gst-libs/gst/riff/riff-media.c in gst-plugins-base in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (floating point exception and crash) via a crafted ASF file.<br>**REFERENCE: CVE-2017-5844** | https://gstreamer.freedesktop.org/releases/1.10/#1.10.3 | A-GST-GSTRE-280217/72 |
| Denial of Service | 09-02-2017 | 4.3 | The html_context_handle_element function in gst/subparse/samiparse.c in gst-plugins-base in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted SMI file, as demonstrated by OneNote_Manager.smi.<br>**REFERENCE: CVE-2017-5842** | https://gstreamer.freedesktop.org/releases/1.10/#1.10.3 | A-GST-GSTRE-280217/73 |
| Denial of | 09-02-2017 | 4.3 | The | https://gstream | A-GST- |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Service | | | gst_riff_create_audio_caps function in gst-libs/gst/riff/riff-media.c in gst-plugins-base in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (floating point exception and crash) via a crafted video file.<br>**REFERENCE: CVE-2017-5837** | er.freedesktop.org/releases/1.10/#1.10.3 | GSTRE-280217/74 |
| Denial of Service | 09-02-2017 | 4.3 | The gst_aac_parse_sink_setcaps function in gst/audioparsers/gstaacparse.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted audio file.<br>**REFERENCE: CVE-2016-10198** | https://gstreamer.freedesktop.org/releases/1.10/#1.10.3 | A-GST-GSTRE-280217/75 |
| Denial of Service | 09-02-2017 | 5 | The gst_ps_demux_parse_psm function in gst/mpegdemux/gstmpegdemux.c in gst-plugins-bad in GStreamer allows remote attackers to cause a denial of service (invalid memory read and crash) via vectors involving PSM parsing.<br>**REFERENCE: CVE-2017-5848** | https://bugzilla.gnome.org/show_bug.cgi?id=777957#c3 | A-GST-GSTRE-280217/76 |
| Denial of Service | 09-02-2017 | 5 | The gst_asf_demux_process_ext_content_desc function in gst/asfdemux/gstasfdemux.c in gst-plugins-ugly in GStreamer allows remote attackers to cause a denial | https://github.com/GStreamer/gst-plugins-ugly/commit/d21017b52a585f145e8d62781bcc1c5fefc7ee37 | A-GST-GSTRE-280217/77 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | of service (out-of-bounds heap read) via vectors involving extended content descriptors. **REFERENCE: CVE-2017-5847** | | |
| Denial of Service | 09-02-2017 | 5 | The gst_avi_demux_parse_ncdt function in gst/avi/gstavidemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (invalid memory read and crash) via a ncdt sub-tag that "goes behind" the surrounding tag. **REFERENCE: CVE-2017-5845** | https://gstreamer.freedesktop.org/releases/1.10/#1.10.3 | A-GST-GSTRE-280217/78 |
| Denial of Service | 09-02-2017 | 5 | Multiple use-after-free vulnerabilities in the (1) gst_mini_object_unref, (2) gst_tag_list_unref, and (3) gst_mxf_demux_update_essence_tracks functions in GStreamer before 1.10.3 allow remote attackers to cause a denial of service (crash) via vectors involving stream tags, as demonstrated by 02785736.mxf. **REFERENCE: CVE-2017-5843** | https://gstreamer.freedesktop.org/releases/1.10/#1.10.3 | A-GST-GSTRE-280217/79 |
| Denial of Service | 09-02-2017 | 5 | The gst_avi_demux_parse_ncdt function in gst/avi/gstavidemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds heap read) via vectors involving ncdt | https://gstreamer.freedesktop.org/releases/1.10/#1.10.3 | A-GST-GSTRE-280217/80 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | tags.<br>**REFERENCE: CVE-2017-5841** |  |  |
| Denial of Service | 09-02-2017 | 5 | The qtdemux_parse_samples function in gst/isomp4/qtdemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds heap read) via vectors involving the current stts index.<br>**REFERENCE: CVE-2017-5840** | https://gstreamer.freedesktop.org/releases/1.10/#1.10.3 | A-GST-GSTRE-280217/81 |
| Denial of Service; Overflow | 09-02-2017 | 5 | The gst_riff_create_audio_caps function in gst-libs/gst/riff/riff-media.c in gst-plugins-base in GStreamer before 1.10.3 does not properly limit recursion, which allows remote attackers to cause a denial of service (stack overflow and crash) via vectors involving nested WAVEFORMATEX.<br>**REFERENCE: CVE-2017-5839** | https://gstreamer.freedesktop.org/releases/1.10/#1.10.3 | A-GST-GSTRE-280217/82 |
| Denial of Service | 09-02-2017 | 5 | The gst_date_time_new_from_iso8601_string function in gst/gstdatetime.c in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a malformed datetime string.<br>**REFERENCE: CVE-2017-5838** | https://gstreamer.freedesktop.org/releases/1.10/#1.10.3 | A-GST-GSTRE-280217/83 |
| Denial of Service | 09-02-2017 | 5 | The qtdemux_tag_add_str_full | https://gstreamer.freedesktop.o | A-GST-GSTRE- |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | function in gst/isomp4/qtdemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted tag value.<br>**REFERENCE: CVE-2016-10199** | rg/releases/1.10/#1.10.3 | 280217/84 |
| **Guac-dev** | | | | | |
| ***Guacamole***<br>Guacamole is a program to control a Linux desktop over the network in a browser. | | | | | |
| Cross Site Scripting | 02-02-2017 | 3.5 | Cross-site scripting (XSS) vulnerability in the file browser in Guacamole 0.9.8 and 0.9.9, when file transfer is enabled to a location shared by multiple users, allows remote authenticated users to inject arbitrary web script or HTML via a crafted filename. NOTE: this vulnerability was fixed in guacamole.war on 2016-01-13, but the version number was not changed.<br>**REFERENCE: CVE-2016-1566** | https://sourceforge.net/p/guacamole/news/2016/02/security-advisory---stored-xss-Reference: CVE-2016-1566--guac-1465/ | A-GUA-GUACA-280217/85 |
| **Hanwha Techwin** | | | | | |
| ***Smart Security Manager***<br>SSM Enterprise is a one-stop, total video management software platform that maximizes the efficiency of Wisenet IP network cameras, recording devices and servers, whilst facilitating integration with third party systems such as intruder alarms and Access Control. | | | | | |
| Execute Code; Cross Site Request Forgery | 13-02-2017 | 5.1 | An issue was discovered in Hanwha Techwin Smart Security Manager Versions 1.5 and prior. Multiple Cross Site Request Forgery vulnerabilities have been identified. The flaws exist within the Redis and Apache Felix Gogo servers | https://ics-cert.us-cert.gov/advisories/ICSA-17-040-01 | A-HAN-SMART-280217/86 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | that are installed as part of this product. By issuing specific HTTP Post requests, an attacker can gain system level access to a remote shell session. Smart Security Manager Versions 1.5 and prior are affected by these vulnerabilities. These vulnerabilities can allow for remote code execution. **REFERENCE: CVE-2017-5169** | | |
| Execute Code; Directory Traversal | 13-02-2017 | 5.1 | An issue was discovered in Hanwha Techwin Smart Security Manager Versions 1.5 and prior. Multiple Path Traversal vulnerabilities have been identified. The flaws exist within the ActiveMQ Broker service that is installed as part of the product. By issuing specific HTTP requests, if a user visits a malicious page, an attacker can gain access to arbitrary files on the server. Smart Security Manager Versions 1.4 and prior to 1.31 are affected by these vulnerabilities. These vulnerabilities can allow for remote code execution. **REFERENCE: CVE-2017-5168** | https://ics-cert.us-cert.gov/advisories/ICSA-17-040-01 | A-HAN-SMART-280217/87 |
| **IBM** | | | | | |
| ***Bigfix Inventory; License Metric Tool***<br>IBM BigFix Inventory provides the foundation for software control and security risk mitigation, with embedded compliance and usage analysis, discovering all licensed and unlicensed software with in-depth granularity across all devices; IBM License Metric Tool helps IBM Passport Advantage customers determine their full and sub-capacity processor value units (PVU) licensing requirements. | | | | | |
| Gain Information | 01-02-2017 | 2.1 | IBM BigFix Inventory v9 allows web pages to be | http://www.ibm.com/support | A-IBM-BIGFI- |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | stored locally which can be read by another user on the system.<br>**REFERENCE: CVE-2016-8981** | /docview.wss?uid=swg21994932 | 280217/88 |
| NA | 01-02-2017 | 2.1 | IBM BigFix Inventory v9 9.2 stores user credentials in plain in clear text which can be read by a local user.<br>**REFERENCE: CVE-2016-8967** | http://www.ibm.com/support/docview.wss?uid=swg21995019 | A-IBM-BIGFI-280217/89 |
| Gain Information | 01-02-2017 | 2.1 | IBM BigFix Inventory v9 stores potentially sensitive information in log files that could be read by a local user.<br>**REFERENCE: CVE-2016-8963** | http://www.ibm.com/support/docview.wss?uid=swg21995029 | A-IBM-BIGFI-280217/90 |
| Gain Information | 01-02-2017 | 4.3 | IBM BigFix Inventory v9 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.<br>**REFERENCE: CVE-2016-8966** | http://www.ibm.com/support/docview.wss?uid=swg21995023 | A-IBM-BIGFI-280217/91 |
| Gain Information | 01-02-2017 | 5 | IBM BigFix Inventory v9 could disclose sensitive information to an unauthorized user using HTTP GET requests. This information could be used to mount further attacks against the system.<br>**REFERENCE: CVE-2016-8977** | http://www.ibm.com/support/docview.wss?uid=swg21995014 | A-IBM-BIGFI-280217/92 |
| Gain Information | 01-02-2017 | 5.8 | IBM BigFix Inventory v9 could allow a remote attacker to conduct | http://www.ibm.com/support/docview.wss?u | A-IBM-BIGFI-280217/93 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim.<br>**REFERENCE: CVE-2016-8961** | id=swg21995037 |  |
| Denial of Service | 01-02-2017 | 7.5 | IBM BigFix Inventory v9 is vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources.<br>**REFERENCE: CVE-2016-8980** | http://www.ibm.com/support/docview.wss?uid=swg21995013 | A-IBM-BIGFI-280217/94 |
| ***Bigfix Platform***<br>IBM BigFix formerly IBM Endpoint Manager, Tivoli Endpoint Manager (TEM) and before that, BigFix, is a systems-management software product developed by IBM for managing large groups of computers running Windows, Mac OS X, VMware ESX, Linux or UNIX, as well as various mobile operating systems such as Windows Phone, Symbian, iOS and Android. |  |  |  |  |  |
| NA | 01-02-2017 | 2.1 | IBM Tivoli Endpoint Manager - Mobile Device Management (MDM) stores potentially sensitive information in log files that could be available to a local user.<br>**REFERENCE: CVE-2016-** | http://www.ibm.com/support/docview.wss?uid=swg21993213 | A-IBM-BIGFI-280217/95 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | **0296** | | |
| NA | 01-02-2017 | 3.3 | IBM BigFix Platform could allow an attacker on the local network to crash the BES and relay servers. **REFERENCE: CVE-2016-6085** | http://www.ibm.com/support/docview.wss?uid=swg21996348 | A-IBM-BIGFI-280217/96 |
| NA | 01-02-2017 | 3.3 | IBM BigFix Platform could allow an attacker on the local network to crash the BES server using a specially crafted XMLSchema request. **REFERENCE: CVE-2016-6084** | http://www.ibm.com/support/docview.wss?uid=swg21996339 | A-IBM-BIGFI-280217/97 |
| Gain Information | 01-02-2017 | 4.3 | IBM Tivoli Endpoint Manager - Mobile Device Management (MDM) could allow a remote attacker to obtain sensitive information due to a missing HTTP Strict-Transport-Security Header through man in the middle techniques. **REFERENCE: CVE-2016-0297** | http://www.ibm.com/support/docview.wss?uid=swg21993214 | A-IBM-BIGFI-280217/98 |
| Execute Code | 01-02-2017 | 6.8 | IBM Tivoli Endpoint Manager could allow a user under special circumstances to inject commands that would be executed with unnecessary higher privileges than expected. **REFERENCE: CVE-2016-0396** | http://www.ibm.com/support/docview.wss?uid=swg21993206 | A-IBM-BIGFI-280217/99 |
| NA | 08-02-2017 | 6.8 | IBM Tivoli Endpoint Manager could allow a remote attacker to upload arbitrary files. A remote attacker could exploit this vulnerability to upload a malicious file. The only way that file would be | http://www.ibm.com/support/docview.wss?uid=swg21993203 | A-IBM-BIGFI-280217/100 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | executed would be through a phishing attack to trick an unsuspecting victim to execute the file.<br>**REFERENCE: CVE-2016-0214** |  |  |
| Execute Code | 01-02-2017 | 10 | IBM BigFix Platform could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free race condition. An attacker could exploit this vulnerability to execute arbitrary code on the system.<br>**REFERENCE: CVE-2016-6082** | http://www.ibm.com/support/docview.wss?uid=swg21996375 | A-IBM-BIGFI-280217/101 |
| ***Biginsights***<br>BigInsights is a collection of value-added services that can be installed on top of the IBM Open Platform with Apache Hadoop, which is the open Hadoop foundation. |  |  |  |  |  |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Infosphere BigInsights is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.<br>**REFERENCE: CVE-2016-2992** | http://www.ibm.com/support/docview.wss?uid=swg21987499 | A-IBM-BIGIN-280217/102 |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Infosphere BigInsights is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the |  http://www.ibm.com/support/docview.wss?uid=swg21987499 | A-IBM-BIGIN-280217/103 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials. **REFERENCE: CVE-2016-2924** | | |
| ***Business Process Manager***<br>IBM Business Process Manager is a full-featured, consumable business process management (BPM) platform. | | | | | |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Business Process Manager is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-9731** | http://www.ibm.com/support/docview.wss?uid=swg21996158 | A-IBM-BUSIN-280217/104 |
| ***Campaign***<br>IBM Campaign, formerly Unica Campaign, provides multichannel marketing campaign management. | | | | | |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Campaign is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials. **REFERENCE: CVE-2016-** | http://www.ibm.com/support/docview.wss?uid=swg21986033 | A-IBM-CAMPA-280217/105 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | **0265** | | |
| ***Client Application Access; Domino; Notes***<br>IBM Client Application Access (formerly known as IBM Notes Browser Plug-in) offers a lightweight solution for accessing your IBM Notes and IBM Domino applications; IBM Domino (formerly IBM Lotus Domino) is an advanced platform for hosting social business applications; IBM Notes, formerly Lotus Notes, is an enterprise email client that integrates messaging, business applications and social collaboration. | | | | | |
| Gain Information | 08-02-2017 | 4.3 | IBM Domino 9.0.1 Fix Pack 3 Interim Fix 2 through 9.0.1 Fix Pack 5 Interim Fix 1, when using TLS and AES GCM, uses random nonce generation, which makes it easier for remote attackers to obtain the authentication key and spoof data by leveraging the reuse of a nonce in a session and a "forbidden attack." NOTE: this CVE has been incorrectly used for GCM nonce reuse issues in other products; see REFERENCE: CVE-2016-10213 for the A10 issue, REFERENCE: CVE-2016-10212 for the Radware issue, and REFERENCE: CVE-2017-5933 for the Citrix issue.<br>**REFERENCE: CVE-2016-0270** | http://www-01.ibm.com/support/docview.wss?uid=swg21979604 | A-IBM-CLIEN-280217/106 |
| ***Cloud Orchestrator***<br>IBM Cloud Orchestrator is a cloud management platform for automating provisioning of cloud services using policy-based tools. | | | | | |
| NA | 08-02-2017 | 2.1 | IBM Cloud Orchestrator could allow a local authenticated attacker to cause the server to slow down for a short period of time by using a specially crafted and malformed URL.<br>**REFERENCE: CVE-2016-0206** | http://www.ibm.com/support/docview.wss?uid=swg2C1000141 | A-IBM-CLOUD-280217/107 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Gain Information | 08-02-2017 | 2.1 | Vulnerability has been identified in tasks, backend object generated for handling any action performed by the application in IBM Cloud Orchestrator. It is possible for an authenticated user to view any task of the current users domain. **REFERENCE: CVE-2016-0202** | http://www.ibm.com/support/docview.wss?uid=swg2C1000134 | A-IBM-CLOUD-280217/108 |
| ***Cloud Orchestrator; Smartcloud Orchestrator***<br>IBM Cloud Orchestrator is a cloud management platform for automating provisioning of cloud services using policy-based tools; IBM SmartCloud Orchestrator V2.3 is a comprehensive open cloud management platform that automates the delivery of cloud services. | | | | | |
| NA | 08-02-2017 | 1.7 | A vulnerability has been identified in IBM Cloud Orchestrator services/[action]/launch API. An authenticated domain admin user might modify cross domain resources via a /services/[action]/launch API call, provided it would have been possible for the domain admin user to gain access to a resource identifier of the other domain. **REFERENCE: CVE-2015-7494** | http://www.ibm.com/support/docview.wss?uid=swg2C1000140 | A-IBM-CLOUD-280217/109 |
| Gain Information | 08-02-2017 | 2.1 | Vulnerability has been identified in the IBM Cloud Orchestrator task API. The task API might allow an authenticated user to view background information associated with actions performed on virtual machines in projects where the user belongs to. **REFERENCE: CVE-2016-0203** | http://www.ibm.com/support/docview.wss?uid=swg2C1000140 | A-IBM-CLOUD-280217/110 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| ***Cognos Analytics***<br>IBM Cognos Analytics offers guided, self-service capabilities designed to solve problems and seize new opportunities quickly. |  |  |  |  |  |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Cognos Business Intelligence and IBM Cognos Analytics are vulnerable to stored cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to inject malicious script into a Web page which would be executed in a victim's Web browser within the security context of the hosting Web site, once the page is viewed. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials. **REFERENCE: CVE-2016-0217** | http://www.ibm.com/support/docview.wss?uid=swg21996417 | A-IBM-COGNO-280217/111 |
| ***Cognos Business Intelligence***<br>IBM Cognos Business Intelligence is a web-based, integrated business intelligence suite by IBM. |  |  |  |  |  |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Cognos TM1 is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials. **REFERENCE: CVE-2016-** | http://www-01.ibm.com/support/docview.wss?uid=swg21995691 | A-IBM-COGNO-280217/112 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | **0218** | | |
| ***Cognos Disclosure Management***<br>IBM Cognos Disclosure Management is a reporting and process automation solution designed to merge financial and operational analytics with narrative analysis in a controlled, auditable environment. | | | | | |
| Execute Code | 15-02-2017 | 6.8 | IBM Cognos Disclosure Management 10.2 could allow a malicious attacker to execute commands as a lower privileged user that opens a malicious document. IBM Reference #: 1991584. **REFERENCE: CVE-2016-6077** | http://www-01.ibm.com/support/docview.wss?uid=swg21991584 | A-IBM-COGNO-280217/113 |
| ***Commerce On Cloud; Websphere Commerce; Websphere Commerce Developer***<br>IBM Commerce on Cloud provides advanced commerce capabilities to help you quickly and easily create an engaging brand experience across every customer touch point; IBM WebSphere Commerce provides an e-commerce platform that can deliver seamless and consistent omni-channel shopping experiences; WebSphere Commerce Developer is the development toolkit for customizing a WebSphere Commerce application. | | | | | |
| Denial of Service | 01-02-2017 | 10 | IBM WebSphere Commerce contains an unspecified vulnerability that could allow disclosure of user personal data, performing of unauthorized administrative operations, and potentially causing a denial of service. **REFERENCE: CVE-2016-6090** | http://www.ibm.com/support/docview.wss?uid=swg21992759 | A-IBM-COMME-280217/114 |
| ***Connections***<br>IBM Connections is a leading business social network platform that helps you get work done. | | | | | |
| Cross Site Scripting | 08-02-2017 | 3.5 | IBM Connections 5.5 and earlier is vulnerable to possible host header injection attack that could cause navigation to the attacker's domain. **REFERENCE: CVE-2016-0310** | http://www.ibm.com/support/docview.wss?uid=swg21988338 | A-IBM-CONNE-280217/115 |
| Cross Site Scripting | 08-02-2017 | 3.5 | IBM Connections is vulnerable to cross-site | http://www.ibm.com/support | A-IBM-CONNE- |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials. **REFERENCE: CVE-2016-0305** | /docview.wss?uid=swg21986770 | 280217/116 |
| NA | 08-02-2017 | 4 | IBM Connections 5.5 and earlier is vulnerable to possible link manipulation attack that could result in the display of inappropriate background images. **REFERENCE: CVE-2016-0308** | http://www.ibm.com/support/docview.wss?uid=swg21986770 | A-IBM-CONNE-280217/117 |
| Gain Information | 08-02-2017 | 4 | IBM Connections 5.5 and earlier allows remote attackers to obtain sensitive information by reading stack traces in returned responses. **REFERENCE: CVE-2016-0307** | http://www.ibm.com/support/docview.wss?uid=swg21986770 | A-IBM-CONNE-280217/118 |
| ***Dashboard Application Services Hub***<br>Dashboard Application Services Hub provides visualization and dashboard services in Jazz for Service Management. | | | | | |
| Gain Information | 02-02-2017 | 4.3 | IBM Jazz for Service Management could allow a remote attacker to obtain sensitive information, caused by the failure to properly validate the SSL certificate. An attacker could exploit this | http://www.ibm.com/support/docview.wss?uid=swg21997711 | A-IBM-DASHB-280217/119 |

| CV Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | vulnerability to obtain sensitive information using man in the middle techniques. **REFERENCE: CVE-2016-5935** |  |  |
| ***Dashdb Local***<br>dashDB Local is next-generation data warehousing and analytics technology for use in private clouds, virtual private clouds and other container-supported infrastructures. |  |  |  |  |  |
| NA | 08-02-2017 | 7.5 | IBM dashDB Local uses hard-coded credentials that could allow a remote attacker to gain access to the Docker container or database. **REFERENCE: CVE-2016-8954** | http://www.ibm.com/support/docview.wss?uid=swg21994471 | A-IBM-DASHD-280217/120 |
| ***Domino; Inotes***<br>IBM Domino (formerly IBM Lotus Domino) is an advanced platform for hosting social business applications; IBM iNotes (formerly IBM Lotus iNotes) offers a full-featured web-based version of IBM's IBM Notes client. |  |  |  |  |  |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM iNotes is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-5880** | http://www.ibm.com/support/docview.wss?uid=swg21992835 | A-IBM-DOMIN-280217/121 |
| Cross Site Scripting | 01-02-2017 | 4.3 | IBM Verse is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-6113** | http://www.ibm.com/support/docview.wss?uid=swg21992835 | A-IBM-DOMIN-280217/122 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Cross Site Scripting | 01-02-2017 | 4.3 | IBM iNotes is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-5884** | http://www.ibm.com/support/docview.wss?uid=swg21992835 | A-IBM-DOMIN-280217/123 |
| Cross Site Scripting | 01-02-2017 | 4.3 | IBM iNotes is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-5882** | http://www.ibm.com/support/docview.wss?uid=swg21992835 | A-IBM-DOMIN-280217/124 |
| Cross Site Scripting | 01-02-2017 | 4.3 | IBM iNotes is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-2939** | http://www.ibm.com/support/docview.wss?uid=swg21992835 | A-IBM-DOMIN-280217/125 |
| Cross Site Scripting | 01-02-2017 | 4.3 | IBM iNotes is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure | http://www.ibm.com/support/docview.wss?uid=swg21992835 | A-IBM-DOMIN-280217/126 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | within a trusted session.<br>**REFERENCE: CVE-2016-2938** | | |
| ***Filenet Workplace Xt***<br>Workplace XT is an optional FileNet P8 platform component (similar to Application Engine) that hosts the Workplace XT web application, providing access to the process and content functionality of FileNet P8. | | | | | |
| Execute Code | 01-02-2017 | 6.5 | IBM FileNet WorkPlace XT could allow a remote attacker to upload arbitrary files, which could allow the attacker to execute arbitrary code on the vulnerable server.<br>**REFERENCE: CVE-2016-8921** | http://www.ibm.com/support/docview.wss?uid=swg21994018 | A-IBM-FILEN-280217/127 |
| ***Forms Experience Builder***<br>IBM Forms Experience Builder empowers business users to create compelling, multi-channel, interactive applications. | | | | | |
| NA | 01-02-2017 | 3.5 | IBM Forms Experience Builder could be susceptible to a server-side request forgery (SSRF) from the application design interface allowing for some information disclosure of internal resources.<br>**REFERENCE: CVE-2016-6001** | http://www.ibm.com/support/docview.wss?uid=swg21991280 | A-IBM-FORMS-280217/128 |
| ***General Parallel File System; Spectrum Scale***<br>IBM Spectrum Scale is a flexible software-defined storage that can be deployed as high performance file storage or a cost optimized large-scale content repository; IBM Spectrum Scale, previously known as IBM General Parallel File System (GPFS), is built from the ground up to scale performance and capacity with no bottlenecks. | | | | | |
| Execute Code; Overflow | 01-02-2017 | 9 | IBM General Parallel File System is vulnerable to a buffer overflow. A remote authenticated attacker could overflow a buffer and execute arbitrary code on the system with root privileges or cause the server to crash. | http://www.ibm.com/support/docview.wss?uid=ssg1S1009639 | A-IBM-GENER-280217/129 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | **REFERENCE: CVE-2016-6115** | | |
| ***Infosphere Datastage***<br>IBM InfoSphere DataStage integrates data across multiple systems using a high performance parallel framework, and it supports extended metadata management and enterprise connectivity. | | | | | |
| Gain Information | 01-02-2017 | 5 | IBM InfoSphere Information Server stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history.<br>**REFERENCE: CVE-2016-8982** | http://www.ibm.com/support/docview.wss?uid=swg21995895 | A-IBM-INFOS-280217/130 |
| ***Infosphere Datastage; Infosphere Information Server; Infosphere Information Server On Cloud***<br>IBM InfoSphere DataStage integrates data across multiple systems using a high performance parallel framework, and it supports extended metadata management and enterprise connectivity; IBM InfoSphere Information Server is a market-leading data integration platform which includes a family of products that enable you to understand, cleanse, monitor, transform, and deliver data, as well as to collaborate to bridge the gap between business and IT. | | | | | |
| Cross Site Scripting | 01-02-2017 | 4.3 | IBM InfoSphere DataStage is vulnerable to cross-frame scripting, caused by insufficient HTML iframe protection. A remote attacker could exploit this vulnerability using a specially-crafted URL to navigate to a web page the attacker controls. An attacker could use this vulnerability to conduct clickjacking or other client-side browser attacks.<br>**REFERENCE: CVE-2016-9000** | http://www.ibm.com/support/docview.wss?uid=swg21995257 | A-IBM-INFOS-280217/131 |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM InfoSphere Information Server contains a Path-relative stylesheet import vulnerability that allows | http://www.ibm.com/support/docview.wss?uid=swg21995155 | A-IBM-INFOS-280217/132 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | attackers to render a page in quirks mode thereby facilitating an attacker to inject malicious CSS. **REFERENCE: CVE-2016-8999** | | |
| Denial of Service | 01-02-2017 | 7.5 | IBM InfoSphere Information Server is vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources. **REFERENCE: CVE-2016-6059** | http://www.ibm.com/support/docview.wss?uid=swg21991683 | A-IBM-INFOS-280217/133 |
| Execute Code; Gain Information | 08-02-2017 | 1.9 | IBM InfoSphere Information Server could allow a local user under special circumstances to execute commands during installation processes that could expose sensitive information. **REFERENCE: CVE-2015-7493** | http://www.ibm.com/support/docview.wss?uid=swg21982034 | A-IBM-INFOS-280217/134 |
| Gain Information | 01-02-2017 | 4 | IBM InfoSphere Information Server contains a vulnerability that would allow an authenticated user to browse any file on the engine tier, and examine its contents. **REFERENCE: CVE-2016-5994** | http://www.ibm.com/support/docview.wss?uid=swg21992171 | A-IBM-INFOS-280217/135 |
| Cross Site Scripting | 01-02-2017 | 4.3 | IBM InfoSphere Information Server is vulnerable to cross-frame scripting, caused by | http://www.ibm.com/support/docview.wss?uid=swg2199168 | A-IBM-INFOS-280217/136 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | insufficient HTML iframe protection. A remote attacker could exploit this vulnerability using a specially-crafted URL to navigate to a web page the attacker controls. An attacker could use this vulnerability to conduct clickjacking or other client-side browser attacks.<br>**REFERENCE: CVE-2016-5984** | 2 | |
| ***Inotes***<br>IBM iNotes (formerly IBM Lotus iNotes) is a web-based email client for IBM Notes. | | | | | |
| Cross Site Scripting | 01-02-2017 | 4.3 | IBM iNotes is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.<br>**REFERENCE: CVE-2016-5881** | http://www.ibm.com/support/docview.wss?uid=swg21995122 | A-IBM-INOTE-280217/137 |
| ***Integration Bus; Websphere Message Broker***<br>IBM Integration Bus is an enterprise service bus (ESB) that offers a fast, simple way for systems and applications to communicate with each other; WebSphere Message Broker is an Enterprise Service Bus (ESB) built for universal connectivity and transformation in heterogeneous IT environments. | | | | | |
| NA | 01-02-2017 | 4.3 | IBM Integration Bus, under non default configurations, could allow a remote user to authenticate without providing valid credentials.<br>**REFERENCE: CVE-2016-8918** | http://www.ibm.com/support/docview.wss?uid=swg21995079 | A-IBM-INTEG-280217/138 |
| NA | 01-02-2017 | 2.1 | IBM Integration Bus and WebSphere Message broker sets incorrect permissions for an object | http://www.ibm.com/support/docview.wss?uid=swg2198501 | A-IBM-INTEG-280217/139 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | that could allow a local attacker to manipulate certain files.<br>**REFERENCE: CVE-2016-0394** | 3 | |
| NA | 15-02-2017 | 4.3 | IBM WebSphere Message Broker 9.0 and 10.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM Reference #: 1997906.<br>**REFERENCE: CVE-2016-9010** | http://www.ibm.com/support/docview.wss?uid=swg21997906 | A-IBM-INTEG-280217/140 |
| Denial of Service | 15-02-2017 | 8.5 | IBM Integration Bus 9.0 and 10.0 and WebSphere Message Broker SOAP FLOWS is vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources. IBM Reference #: 1997918.<br>**REFERENCE: CVE-2016-9706** | http://www.ibm.com/support/docview.wss?uid=swg21997918 | A-IBM-INTEG-280217/141 |

***Jazz Reporting Service***

IBM Jazz Reporting Service is an alternative to the complex reporting capabilities that are available in many Rational products and solutions. The Jazz Reporting Service creates reports from the tools in the IBM Rational solution for Collaborative Lifecycle Management (CLM). It is designed for non-technical practitioners who simply want to find information about their software projects and socialize that information in their enterprise through dashboards.

| CV Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Jazz Foundation is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-6054** | http://www.ibm.com/support/docview.wss?uid=swg21991154 | A-IBM-JAZZ-280217/142 |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Jazz Reporting Service (JRS) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-6047** | http://www.ibm.com/support/docview.wss?uid=swg21991154 | A-IBM-JAZZ-280217/143 |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Jazz Reporting Service (JRS) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-6039** | http://www.ibm.com/support/docview.wss?uid=swg21991153 | A-IBM-JAZZ-280217/144 |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Jazz Reporting Service (JRS) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web | http://www.ibm.com/support/docview.wss?uid=swg21991154 | A-IBM-JAZZ-280217/145 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-5899** | | |
| Execute Code; Cross Site Scripting | 01-02-2017 | 3.5 | IBM Jazz Reporting Service (JRS) is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. **REFERENCE: CVE-2016-5897** | http://www.ibm.com/support/docview.wss?uid=swg21991153 | A-IBM-JAZZ-280217/146 |
| Gain Information | 01-02-2017 | 4 | IBM Jazz Reporting Service (JRS) could allow a remote attacker to obtain sensitive information, caused by not restricting JSON serialization. By sending a direct request, an attacker could exploit this vulnerability to obtain sensitive information. **REFERENCE: CVE-2016-5898** | http://www.ibm.com/support/docview.wss?uid=swg21991154 | A-IBM-JAZZ-280217/147 |
| ***Kenexa Lcms Premier***<br>IBM Kenexa LCMS Premier on Cloud enables organizations to develop and optimize content to help meet business objectives and goals. | | | | | |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Kenexa LCMS Premier on Cloud is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. | http://www.ibm.com/support/docview.wss?uid=swg21992067 | A-IBM-KENEX-280217/148 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | **REFERENCE: CVE-2016-5951** | | |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Kenexa LCMS Premier on Cloud is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-5948** | http://www.ibm.com/support/docview.wss?uid=swg21992067 | A-IBM-KENEX-280217/149 |
| NA | 01-02-2017 | 4 | IBM Kenexa LCMS Premier on Cloud stores user credentials in plain in clear text which can be read by an authenticated user. **REFERENCE: CVE-2016-5950** | http://www.ibm.com/support/docview.wss?uid=swg21992067 | A-IBM-KENEX-280217/150 |
| NA | 01-02-2017 | 4 | IBM Kenexa LCMS Premier on Cloud could allow an authenticated user to obtain sensitive user data with a specially crafted HTTP request. **REFERENCE: CVE-2016-5949** | http://www.ibm.com/support/docview.wss?uid=swg21992276 | A-IBM-KENEX-280217/151 |
| SQL Injection | 01-02-2017 | 6.5 | IBM Kenexa LCMS Premier on Cloud is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. **REFERENCE: CVE-2016-5952** | http://www.ibm.com/support/docview.wss?uid=swg21976805 | A-IBM-KENEX-280217/152 |
| Cross Site Request | 01-02-2017 | 6.8 | IBM Kenexa LCMS Premier on Cloud is vulnerable to | http://www.ibm.com/support | A-IBM-KENEX- |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| Forgery |  |  | cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.<br>**REFERENCE: CVE-2016-5937** | /docview.wss?uid=swg21992067 | 280217/153 |
| ***Kenexa Lms***<br>IBM Kenexa LMS on Cloud enables organizations to seamlessly integrate both formal and social learning into a comprehensive learning and performance support strategy. |  |  |  |  |  |
| Gain Information | 01-02-2017 | 2.1 | IBM Kenexa LMS on Cloud allows web pages to be stored locally which can be read by another user on the system.<br>**REFERENCE: CVE-2016-5938** | http://www.ibm.com/support/docview.wss?uid=swg21992072 | A-IBM-KENEX-280217/154 |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Kenexa LMS on Cloud is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.<br>**REFERENCE: CVE-2016-5942** | http://www.ibm.com/support/docview.wss?uid=swg21992072 | A-IBM-KENEX-280217/155 |
| Directory Traversal | 01-02-2017 | 3.5 | IBM Kenexa LMS on Cloud could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing dot dot sequences (/../) to view arbitrary files on the system.<br>**REFERENCE: CVE-2016-5941** | http://www.ibm.com/support/docview.wss?uid=swg21992072 | A-IBM-KENEX-280217/156 |
| Cross Site | 01-02-2017 | 3.5 | IBM Kenexa LMS on Cloud | http://www.ib | A-IBM- |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Scripting | | | is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-5940** | m.com/support/docview.wss?uid=swg21992072 | KENEX-280217/157 |
| Directory Traversal | 01-02-2017 | 4 | IBM Kenexa LMS on Cloud could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing dot dot sequences (/../) to view arbitrary files on the system. **REFERENCE: CVE-2016-8933** | http://www.ibm.com/support/docview.wss?uid=swg21992072 | A-IBM-KENEX-280217/158 |
| SQL Injection | 01-02-2017 | 5.5 | IBM Kenexa LMS on Cloud is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. **REFERENCE: CVE-2016-8929** | http://www.ibm.com/support/docview.wss?uid=swg21992072 | A-IBM-KENEX-280217/159 |
| Execute Code | 01-02-2017 | 6.5 | IBM Kenexa LMS on Cloud could allow a remote attacker to upload arbitrary files, which could allow the attacker to execute arbitrary code on the vulnerable server. **REFERENCE: CVE-2016-8932** | http://www.ibm.com/support/docview.wss?uid=swg21992072 | A-IBM-KENEX-280217/160 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Execute Code | 01-02-2017 | 6.5 | IBM Kenexa LMS on Cloud could allow a remote attacker to upload arbitrary files, which could allow the attacker to execute arbitrary code on the vulnerable server.<br>**REFERENCE: CVE-2016-8931** | http://www.ibm.com/support/docview.wss?uid=swg21992072 | A-IBM-KENEX-280217/161 |
| SQL Injection | 01-02-2017 | 6.5 | IBM Kenexa LMS on Cloud is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database.<br>**REFERENCE: CVE-2016-8930** | http://www.ibm.com/support/docview.wss?uid=swg21992072 | A-IBM-KENEX-280217/162 |
| SQL Injection | 01-02-2017 | 6.5 | IBM Kenexa LMS on Cloud is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database.<br>**REFERENCE: CVE-2016-8928** | http://www.ibm.com/support/docview.wss?uid=swg21992072 | A-IBM-KENEX-280217/163 |
| SQL Injection | 01-02-2017 | 6.5 | IBM Kenexa LMS on Cloud is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database.<br>**REFERENCE: CVE-2016-5939** | http://www.ibm.com/support/docview.wss?uid=swg21992129 | A-IBM-KENEX-280217/164 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| ***Kenexa Lms On Cloud***<br>IBM Kenexa LMS on Cloud enables organizations to seamlessly integrate both formal and social learning into a comprehensive learning and performance support strategy. | | | | | |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Kenexa LMS on Cloud 13.1 and 13.2 - 13.2.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-8920** | http://www.ibm.com/support/docview.wss?uid=swg21993982 | A-IBM-KENEX-280217/165 |
| ***Kenexa Lms On Cloud***<br>IBM Kenexa LMS on Cloud enables organizations to seamlessly integrate both formal and social learning into a comprehensive learning and performance support strategy. | | | | | |
| NA | 01-02-2017 | 3.5 | IBM Kenexa LMS on Cloud 13.1 and 13.2 - 13.2.4 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. **REFERENCE: CVE-2016-8911** | http://www.ibm.com/support/docview.wss?uid=swg21993982 | A-IBM-KENEX-280217/166 |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Kenexa LMS on Cloud 13.1 and 13.2 - 13.2.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to | http://www.ibm.com/support/docview.wss?uid=swg21993982 | A-IBM-KENEX-280217/167 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | credentials disclosure within a trusted session. **REFERENCE: CVE-2016-6125** | | |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Kenexa LMS on Cloud 13.1 and 13.2 - 13.2.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-6123** | http://www.ibm.com/support/docview.wss?uid=swg21993982 | A-IBM-KENEX-280217/168 |
| Directory Traversal | 01-02-2017 | 4 | IBM Kenexa LMS on Cloud 13.1 and 13.2 - 13.2.4 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. **REFERENCE: CVE-2016-8913** | http://www.ibm.com/support/docview.wss?uid=swg21993982 | A-IBM-KENEX-280217/169 |
| NA | 01-02-2017 | 4 | IBM Kenexa LMS on Cloud 13.1 and 13.2 - 13.2.4 stores potentially sensitive information in in log files that could be read by an authenticated user. **REFERENCE: CVE-2016-8912** | http://www.ibm.com/support/docview.wss?uid=swg21993982 | A-IBM-KENEX-280217/170 |
| Directory Traversal | 01-02-2017 | 4 | IBM Kenexa LMS on Cloud 13.1 and 13.2 - 13.2.4 could allow a remote attacker to traverse directories on the system. An attacker could send a | http://www.ibm.com/support/docview.wss?uid=swg21993982 | A-IBM-KENEX-280217/171 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.<br>**REFERENCE: CVE-2016-6126** | | |
| Gain Information | 01-02-2017 | 4 | IBM Kenexa LMS on Cloud 13.1 and 13.2 - 13.2.4 discloses answers to security questions in a response to authenticated users.<br>**REFERENCE: CVE-2016-6122** | http://www.ibm.com/support/docview.wss?uid=swg21993982 | A-IBM-KENEX-280217/172 |
| Execute Code | 01-02-2017 | 6.5 | IBM Kenexa LMS on Cloud 13.1 and 13.2 - 13.2.4 could allow a remote attacker to upload arbitrary files, which could allow the attacker to execute arbitrary code on the vulnerable server.<br>**REFERENCE: CVE-2016-6124** | http://www.ibm.com/support/docview.wss?uid=swg21993982 | A-IBM-KENEX-280217/173 |

***Maximo Asset Management; Maximo For Aviation; Maximo For Energy Optimization; Maximo For Government; Maximo For Life Sciences; Maximo For Nuclear Power; Maximo For Oil And Gas; Maximo For Transportation; Maximo For Utilities***

IBM Maximo Asset Management is a comprehensive solution for managing physical assets on a common platform in asset-intensive industries. It offers “built in” mobile access, out-of-the box mapping, crew management and analytical insight; IBM Maximo for Aviation creates greater insight into the health of the many components of an airplane; Optimize energy efficiency of assets with IBM Maximo Asset Management for Energy Optimization; IBM Maximo for Government is a system that is compliant with Federal Acquisition Regulation (FAR) requirements; IBM Maximo for Life Sciences is an integrated asset management system for managing tools, equipment, facilities, mobile & IT assets across the enterprise; IBM Maximo for Nuclear Power is an enterprise asset management system that provides a single platform for managing the assets of nuclear plants and fleets; Maximo for Oil and Gas is a complete enterprise asset management solution that helps manage production equipment, facilities, transportation and infrastructure assets on a single, integrated platform; IBM Maximo for Transportation provides enterprise asset management best practices to improve the productivity of all types of transportation assets; IBM Maximo for Utilities offers a complete solution for work and asset management across business units, including gas and electrical transmission, distribution, power generation, water treatment, and wastewater treatment in a single platform and database.

| | | | | | |
|---|---|---|---|---|---|
| Cross Site Scripting | 08-02-2017 | 4.3 | IBM Maximo Asset Management is vulnerable | http://www.ibm.com/support | A-IBM-MAXIM- |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-5902** | /docview.wss?uid=swg21988252 | 280217/174 |
| Gain Information | 01-02-2017 | 5 | IBM Maximo Asset Management could disclose sensitive information from a stack trace after submitting incorrect login onto Cognos browser. **REFERENCE: CVE-2016-5896** | http://www.ibm.com/support/docview.wss?uid=swg21987855 | A-IBM-MAXIM-280217/175 |
| ***Maximo Asset Management; Maximo For Aviation; Maximo For Life Sciences; Maximo For Nuclear Power;Maximo For Oil And Gas;Maximo For Transportation; Maximo For Utilities; Smartcloud Control Desk; Tivoli Asset Management For It; Tivoli Change And Configuration Management Database; Tivoli Integration Composer; Tivoli Service Request Manager***<br>IBM Maximo Asset Management is a comprehensive solution for managing physical assets on a common platform in asset-intensive industries. It offers “built in” mobile access, out-of-the box mapping, crew management and analytical insight; IBM Maximo for Aviation creates greater insight into the health of the many components of an airplane; Optimize energy efficiency of assets with IBM Maximo Asset Management for Energy Optimization; IBM Maximo for Government is a system that is compliant with Federal Acquisition Regulation (FAR) requirements; IBM Maximo for Life Sciences is an integrated asset management system for managing tools, equipment, facilities, mobile & IT assets across the enterprise; IBM Maximo for Nuclear Power is an enterprise asset management system that provides a single platform for managing the assets of nuclear plants and fleets; Maximo for Oil and Gas is a complete enterprise asset management solution that helps manage production equipment, facilities, transportation and infrastructure assets on a single, integrated platform; IBM Maximo for Transportation provides enterprise asset management best practices to improve the productivity of all types of transportation assets; IBM Maximo for Utilities offers a complete solution for work and asset management across business units, including gas and electrical transmission, distribution, power generation, water treatment, and wastewater treatment in a single platform and database. | | | | | |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Maximo Asset Management is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web | http://www.ibm.com/support/docview.wss?uid=swg21991893 | A-IBM-MAXIM-280217/176 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-6072** |  |  |
| ***Rational Collaborative Lifecycle Management***<br>The Rational solution for Collaborative Lifecycle Management (CLM) is a set of seamlessly integrated tools that work together as one. |  |  |  |  |  |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Jazz Foundation is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-6061** | https://www.ibm.com/support/docview.wss?uid=swg21996097 | A-IBM-RATIO-280217/177 |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Jazz Foundation is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-6030** | https://www.ibm.com/support/docview.wss?uid=swg21996097 | A-IBM-RATIO-280217/178 |
| Cross Site Scripting | 08-02-2017 | 3.5 | IBM Rational Team Concert 4.0, 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality | http://www.ibm.com/support/docview.wss?uid=swg21997104 | A-IBM-RATIO-280217/179 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-6032** |  |  |
| Cross Site Scripting | 15-02-2017 | 3.5 | IBM Jazz Foundation is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1998515. **REFERENCE: CVE-2016-8968** | http://www.ibm.com/support/docview.wss?uid=swg21998515 | A-IBM-RATIO-280217/180 |
| NA | 01-02-2017 | 4 | IBM Jazz technology based products might allow an attacker to view work item titles that they do not have privilege to view. **REFERENCE: CVE-2016-6028** | https://www.ibm.com/support/docview.wss?uid=swg21996097 | A-IBM-RATIO-280217/181 |
| Gain Information | 08-02-2017 | 4 | An unspecified vulnerability in IBM Jazz Team Server may disclose some deployment information to an authenticated user. **REFERENCE: CVE-2016-2866** | http://www.ibm.com/support/docview.wss?uid=swg21997104 | A-IBM-RATIO-280217/182 |
| NA | 01-02-2017 | 6 | IBM Jazz Foundation could allow an authenticated user to take over a previously logged in user due to session expiration not being enforced. **REFERENCE: CVE-2016-6040** | https://www.ibm.com/support/docview.wss?uid=swg21996097 | A-IBM-RATIO-280217/183 |
| ***Rational Doors Next Generation;Rational Engineering Lifecycle Manager;Rational Quality Manager;Rational Rhapsody Design Manager;Rational Software Architect Design*** |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| ***Manager;Rational Team Concert***<br>IBM Rational DOORS Next Generation is a requirements management tool that provides a smarter way to define, trace, analyze, and manage requirements; IBM Rational Engineering Lifecycle Manager visualizes, analyzes and organizes engineering lifecycle data and data relationships; Rational Quality Manager is a test management tool. It stores test cases, records test execution and results, m aps testing onto requirements and tracks defects; IBM Rational Rhapsody Design Manager is collaborative design management software that helps design teams and their stakeholders to share, trace, review and manage designs. Supporting the systems engineering and embedded software development lifecycle, Rational Rhapsody Design Manager helps to effectively manage complexity, reduce risk and improve systems engineering and software quality, design and delivery; IBM Rational Software Architect Design Manager is a collaborative software development and design platform built on Jazz technology; Rational Team Concert is a software development team collaboration tool developed by the Rational Software brand of IBM, who first released it in 2008. | | | | | |
| Gain Information | 01-02-2017 | 4 | An undisclosed vulnerability in CLM applications may result in some administrative deployment parameters being shown to an attacker.<br>**REFERENCE: CVE-2016-2987** | https://www.ibm.com/support/docview.wss?uid=swg21996097 | A-IBM-RATIO-280217/184 |
| ***Rational Doors Next Generation; Rational Requirements Composer***<br>IBM Rational DOORS Next Generation is a requirements management tool that provides a smarter way to define, trace, analyze, and manage requirements; IBM Rational Requirements Composer software empowers teams to define, manage and report on requirements in a lifecycle development project. | | | | | |
| Cross Site Scripting | 08-02-2017 | 3.5 | IBM Rational DOORS Next Generation 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.<br>**REFERENCE: CVE-2017-1128** | http://www.ibm.com/support/docview.wss?uid=swg21996645 | A-IBM-RATIO-280217/185 |
| Cross Site Scripting | 08-02-2017 | 3.5 | IBM Rational DOORS Next Generation 4.0, 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users | http://www.ibm.com/support/docview.wss?uid=swg21996645 | A-IBM-RATIO-280217/186 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.<br>**REFERENCE: CVE-2017-1127** | | |
| Gain Information | 08-02-2017 | 4 | IBM Rational DOORS Next Generation 5.0 and 6.0 discloses sensitive information in error response messages that could be used for further attacks against the system.<br>**REFERENCE: CVE-2016-9748** | http://www.ibm.com/support/docview.wss?uid=swg21991461 | A-IBM-RATIO-280217/187 |
| Gain Information | 15-02-2017 | 4 | An undisclosed vulnerability in IBM Rational DOORS Next Generation 4.0, 5.0, and 6.0 could allow a JazzGuest user to see project names. IBM Reference #: 1995547.<br>**REFERENCE: CVE-2016-6060** | http://www.ibm.com/support/docview.wss?uid=swg21995547 | A-IBM-RATIO-280217/188 |
| ***Security Access Manager; Security Access Manager For Mobile; Security Access Manager For Web***<br>IBM Security Access Manager integrated appliance is designed to manage Access in the world of Hybrid Cloud & enable SSO and identity federation to apps running inside & outside of the enterprise. | | | | | |
| Gain Information | 01-02-2017 | 4.3 | IBM Security Access Manager for Web stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referer header or browser history.<br>**REFERENCE: CVE-2016-3045** | http://www.ibm.com/support/docview.wss?uid=swg21995435 | A-IBM-SECUR-280217/189 |
| Cross Site Scripting | 01-02-2017 | 4.3 | IBM Security Access Manager for Web is | http://www.ibm.com/support | A-IBM-SECUR- |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-3018** | /docview.wss?uid=swg21995347 | 280217/190 |
| ***Security Appscan***<br>IBM Security AppScan Standard helps organizations decrease the likelihood of web application attacks and costly data breaches by automating application security vulnerability testing. |  |  |  |  |  |
| Execute Code; Overflow | 01-02-2017 | 9.3 | IBM AppScan Enterprise Edition could allow a remote attacker to execute arbitrary code on the system, caused by improper handling of objects in memory. By persuading a victim to open specially-crafted content, an attacker could exploit this vulnerability to execute arbitrary code on the system in the same context as the victim. **REFERENCE: CVE-2016-6042** | http://www.ibm.com/support/docview.wss?uid=swg21995118 | A-IBM-SECUR-280217/191 |
| ***Security Appscan Source***<br>IBM Security AppScan Source delivers maximum value to every user in your organization who plays a role in software security. |  |  |  |  |  |
| NA | 01-02-2017 | 2.1 | IBM AppScan Source uses a one-way hash without salt to encrypt highly sensitive information, which could allow a local attacker to decrypt information more easily. **REFERENCE: CVE-2016-3034** | http://www.ibm.com/support/docview.wss?uid=swg21995903 | A-IBM-SECUR-280217/192 |
| Gain Information | 01-02-2017 | 5 | IBM AppScan Source could reveal some sensitive | http://www.ibm.com/support | A-IBM-SECUR- |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | information through the browsing of testlinks on the server.<br>**REFERENCE: CVE-2016-3035** | /docview.wss?uid=swg21987325 | 280217/193 |
| ***Security Directory Server;Tivoli Directory Server***<br>IBM Security Directory Server is an enterprise directory for corporate intranets and the Internet; IBM Security Directory Server, formerly known as IBM Directory Server and IBM Tivoli Directory Server, is an IBM implementation of the Lightweight Directory Access Protocol. | | | | | |
| Execute Code | 08-02-2017 | 2.1 | IBM Security Directory Server could allow an authenticated user to execute commands into the web administration tool that would cause the tool to crash.<br>**REFERENCE: CVE-2015-1976** | http://www.ibm.com/support/docview.wss?uid=swg21980585 | A-IBM-SECUR-280217/194 |
| ***Security Guardium***<br>IBM Security Guardium products help to ensure the security, privacy and integrity of information in your data center. | | | | | |
| Execute Code | 01-02-2017 | 7.2 | IBM Security Guardium Database Activity Monitor appliance could allow a local user to inject commands that would be executed as root.<br>**REFERENCE: CVE-2016-6065** | http://www.ibm.com/support/docview.wss?uid=swg21995657 | A-IBM-SECUR-280217/195 |
| ***Security Identity Manager Virtual Appliance***<br>NA | | | | | |
| NA | 01-02-2017 | 2.1 | IBM Security Identity Manager Virtual Appliance stores user credentials in plain in clear text which can be read by a local user.<br>**REFERENCE: CVE-2016-9739** | http://www.ibm.com/support/docview.wss?uid=swg21996761 | A-IBM-SECUR-280217/196 |
| Gain Information | 01-02-2017 | 2.1 | IBM Security Identity Manager Virtual Appliance does not invalidate session tokens which could allow an unauthorized user with physical access to the | http://www.ibm.com/support/docview.wss?uid=swg21996761 | A-IBM-SECUR-280217/197 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | work station to obtain sensitive information.<br>**REFERENCE: CVE-2016-9703** | | |
| Cross Site Scripting | 01-02-2017 | 4.3 | IBM Security Identity Manager Virtual Appliance is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.<br>**REFERENCE: CVE-2016-9704** | http://www.ibm.com/support/docview.wss?uid=swg21996761 | A-IBM-SECUR-280217/198 |
| ***Security Key Lifecycle Manager***<br>IBM Security Key Lifecycle Manager, formerly Tivoli Key Lifecycle Manager, centralizes, simplifies and automates the encryption key management process to help minimize risk and reduce operational costs of encryption key management. It offers secure and robust key storage, key serving and key lifecycle management for IBM and non-IBM storage solutions using the OASIS Key Management Interoperability Protocol (KMIP). | | | | | |
| Gain Information | 02-02-2017 | 4.3 | IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.<br>**REFERENCE: CVE-2016-6116** | http://www.ibm.com/support/docview.wss?uid=swg21997805 | A-IBM-SECUR-280217/199 |
| Gain Information | 01-02-2017 | 5 | IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 can be deployed with active debugging code that can disclose sensitive information.<br>**REFERENCE: CVE-2016-** | http://www.ibm.com/support/docview.wss?uid=swg21997983 | A-IBM-SECUR-280217/200 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | **6117** | | |
| Gain Information | 02-02-2017 | 5 | IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system.<br>**REFERENCE: CVE-2016-6099** | http://www.ibm.com/support/docview.wss?uid=swg21997924 | A-IBM-SECUR-280217/201 |
| NA | 02-02-2017 | 5 | IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials.<br>**REFERENCE: CVE-2016-6095** | http://www.ibm.com/support/docview.wss?uid=swg21997802 | A-IBM-SECUR-280217/202 |
| NA | 01-02-2017 | 6.4 | IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 do not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas.<br>**REFERENCE: CVE-2016-6105** | http://www.ibm.com/support/docview.wss?uid=swg21997741 | A-IBM-SECUR-280217/203 |
| Execute Code | 07-02-2017 | 6.5 | IBM Tivoli Key Lifecycle Manager 2.5, and 2.6 could allow a remote attacker to upload arbitrary files, caused by the improper validation of file extensions, which could allow the attacker to execute arbitrary code on the vulnerable system.<br>**REFERENCE: CVE-2016-6104** | http://www.ibm.com/support/docview.wss?uid=swg21997988 | A-IBM-SECUR-280217/204 |
| Cross Site Request Forgery | 02-02-2017 | 6.8 | IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 is vulnerable to cross-site | http://www.ibm.com/support/docview.wss?u | A-IBM-SECUR-280217/205 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. **REFERENCE: CVE-2016-6103** | id=swg21997949 | |
| ***Security Key Lifecycle Manager;Tivoli Key Lifecycle Manager***<br>IBM Security Key Lifecycle Manager, formerly Tivoli Key Lifecycle Manager, centralizes, simplifies and automates the encryption key management process to help minimize risk and reduce operational costs of encryption key management. It offers secure and robust key storage, key serving and key lifecycle management for IBM and non-IBM storage solutions using the OASIS Key Management Interoperability Protocol (KMIP). | | | | | |
| Gain Information | 07-02-2017 | 2.1 | IBM Tivoli Key Lifecycle Manager 2.0.1, 2.5, and 2.6 allows web pages to be stored locally which can be read by another user on the system. **REFERENCE: CVE-2016-6097** | http://www.ibm.com/support/docview.wss?uid=swg21997986 | A-IBM-SECUR-280217/206 |
| Gain Information | 07-02-2017 | 2.1 | IBM Tivoli Key Lifecycle Manager 2.0.1, 2.5, and 2.6 stores user credentials in plain in clear text which can be read by a local user. **REFERENCE: CVE-2016-6092** | http://www.ibm.com/support/docview.wss?uid=swg21997953 | A-IBM-SECUR-280217/207 |
| Gain Information | 07-02-2017 | 4 | IBM Tivoli Key Lifecycle Manager 2.0.1, 2.5, and 2.6 generates an error message that includes sensitive information about its environment, users, or associated data. **REFERENCE: CVE-2016-6094** | http://www.ibm.com/support/docview.wss?uid=swg21997987 | A-IBM-SECUR-280217/208 |
| Cross Site Scripting | 07-02-2017 | 4.3 | IBM Tivoli Key Lifecycle Manager 2.0.1, 2.5, and 2.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web | http://www.ibm.com/support/docview.wss?uid=swg21997984 | A-IBM-SECUR-280217/209 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-6096** | | |
| ***Security Privileged Identity Manager***<br>IBM Security Privileged Identity Manager secures, automates and audits the use of privileged identities to help thwart insider attacks and improve security. | | | | | |
| Gain Information | 01-02-2017 | 4 | IBM Security Privileged Identity Manager Virtual Appliance could disclose sensitive information in generated error messages that would be available to an authenticated user. **REFERENCE: CVE-2016-5988** | http://www.ibm.com/support/docview.wss?uid=swg21996614 | A-IBM-SECUR-280217/210 |
| Gain Information | 01-02-2017 | 4.3 | IBM Security Privileged Identity Manager Virtual Appliance could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. **REFERENCE: CVE-2016-5966** | http://www.ibm.com/support/docview.wss?uid=swg21996614 | A-IBM-SECUR-280217/211 |
| NA | 01-02-2017 | 5 | IBM Security Privileged Identity Manager Virtual Appliance version 2.0.2 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. **REFERENCE: CVE-2016-5964** | http://www.ibm.com/support/docview.wss?uid=swg21994065 | A-IBM-SECUR-280217/212 |
| Gain | 01-02-2017 | 5 | IBM Security Privileged | http://www.ib | A-IBM- |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Information | | | Identity Manager could allow a remote attacker to obtain sensitive information, caused by the failure to set the secure flag for the session cookie in SSL mode. By intercepting its transmission within an HTTP session, an attacker could exploit this vulnerability to capture the cookie and obtain sensitive information. **REFERENCE: CVE-2016-5958** | m.com/support/docview.wss?uid=swg21996614 | SECUR-280217/213 |
| NA | 01-02-2017 | 6.5 | IBM Security Privileged Identity Manager Virtual Appliance allows an authenticated user to upload malicious files that would be automatically executed by the server. **REFERENCE: CVE-2016-5990** | http://www.ibm.com/support/docview.wss?uid=swg21996614 | A-IBM-SECUR-280217/214 |
| ***Social Rendering Templates For Digital Data Connector***<br>The IBM Social Rendering Templates for Digital Data Connector package contains a set of web content libraries, sample pages, page templates and new portlets that use the provided web content to integrate social data from IBM Connections into WebSphere Portal. | | | | | |
| Cross Site Scripting | 01-02-2017 | 4.3 | IBM Social Rendering Templates for Digital Data Connector is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-8936** | http://www.ibm.com/support/docview.wss?uid=swg21993895 | A-IBM-SOCIA-280217/215 |
| ***Spectrum Control; Tivoli Storage Productivity Center***<br>IBM Spectrum Control is a comprehensive solution that can significantly improve monitoring, | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| automation and analytics capabilities in multi-vendor storage environments; IBM Tivoli Storage Productivity Center Suite is an integrated storage infrastructure management suite. | | | | | |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Tivoli Storage Productivity Center is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-8943** | http://www.ibm.com/support/docview.wss?uid=swg21995128 | A-IBM-SPECT-280217/216 |
| NA | 01-02-2017 | 3.5 | IBM Tivoli Storage Productivity Center could allow an authenticated user with intimate knowledge of the system to edit a limited set of properties on the server. **REFERENCE: CVE-2016-8942** | http://www.ibm.com/support/docview.wss?uid=swg21995128 | A-IBM-SPECT-280217/217 |
| Cross Site Request Forgery | 01-02-2017 | 6.8 | IBM Tivoli Storage Productivity Center is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. **REFERENCE: CVE-2016-8941** | http://www.ibm.com/support/docview.wss?uid=swg21995128 | A-IBM-SPECT-280217/218 |
| ***Sterling B2b Integrator***<br>IBM Sterling B2B Integrator enables the security-rich integration of complex B2B processes with diverse partner communities. | | | | | |
| Gain Information | 08-02-2017 | 5 | IBM Sterling B2B Integrator Standard Edition could allow a remote attacker to obtain sensitive information. By allowing HTTP OPTIONS | http://www.ibm.com/support/docview.wss?uid=swg21981549 | A-IBM-STERL-280217/219 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | method, a remote attacker could send a specially-crafted query to a vulnerable server running to cause the server to disclose sensitive information in the HTTP response.<br>**REFERENCE: CVE-2016-0210** | | |
| Gain Information | 01-02-2017 | 5.8 | IBM Sterling B2B Integrator Standard Edition could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim.<br>**REFERENCE: CVE-2016-6020** | http://www.ibm.com/support/docview.wss?uid=swg21995794 | A-IBM-STERL-280217/220 |
| ***Sterling Selling And Fulfillment Foundation***<br>NA | | | | | |
| Gain Information | 01-02-2017 | 4.3 | IBM Sterling Order Management transmits the session identifier within the URL. When a user is unable to view a certain view due to not being allowed permissions, the website responds with an error page where the session identifier is encoded as Base64 in the | http://www.ibm.com/support/docview.wss?uid=swg21994521 | A-IBM-STERL-280217/221 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | URL.<br>**REFERENCE: CVE-2016-5953** | | |
| ***System Storage Ts3100-ts3200 Tape Library***<br>The IBM System Storage TS3100 and TS3200 Tape Libraries are well-suited for handling the backup, restore, and archive data-storage needs for small-to-medium environments. | | | | | |
| NA | 08-02-2017 | 7.5 | IBM System Storage TS3100-TS3200 Tape Library could allow an unauthenticated user with access to the company network, to change a user's password and gain remote access to the system.<br>**REFERENCE: CVE-2016-9005** | http://www.ibm.com/support/docview.wss?uid=ssg1S1009656 | A-IBM-SYSTE-280217/222 |
| ***Tealeaf Customer Experience On Cloud Network Capture Add-on***<br>IBM Tealeaf Customer Experience on Cloud delivers IBM Tealeaf core capabilities in an IBM managed cloud environment. | | | | | |
| Gain Information | 08-02-2017 | 4.3 | IBM Tealeaf Customer Experience on Cloud Network Capture Add-On could allow a remote attacker to obtain sensitive information, caused by the failure to properly validate the TLS certificate. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.<br>**REFERENCE: CVE-2016-5900** | http://www.ibm.com/support/docview.wss?uid=swg21994534 | A-IBM-TEALE-280217/223 |
| ***Tivoli Storage Flashcopy Manager For Vmware; Tivoli Storage Manager For Virtual Environments Data Protection For Vmware***<br>IBM Spectrum Protect (Tivoli Storage Manager) is a data protection platform that gives enterprises a single point of control and administration for backup and recovery. | | | | | |
| Cross Site Request Forgery | 15-02-2017 | 6.8 | IBM Tivoli Storage Manager for Virtual Environments 7.1 (VMware) is vulnerable to cross-site request forgery | http://www.ibm.com/support/docview.wss?uid=swg21995545 | A-IBM-TIVOL-280217/224 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM Reference #: 1995545.<br>**REFERENCE: CVE-2016-6033** | | |
| ***Tivoli Storage Manager***<br>IBM Spectrum Protect (Tivoli Storage Manager) is a data protection platform that gives enterprises a single point of control and administration for backup and recovery. | | | | | |
| Gain Information | 01-02-2017 | 1.9 | The Tivoli Storage Manager (TSM) password may be displayed in plain text via application trace output while application tracing is enabled.<br>**REFERENCE: CVE-2016-0371** | http://www-01.ibm.com/support/docview.wss?uid=swg21985114 | A-IBM-TIVOL-280217/225 |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM Tivoli Storage Manager Operations Center is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.<br>**REFERENCE: CVE-2016-6046** | http://www.ibm.com/support/docview.wss?uid=swg21995754 | A-IBM-TIVOL-280217/226 |
| NA | 01-02-2017 | 4 | IBM Tivoli Storage Manager Operations Center could allow an authenticated attacker to enable or disable the application's REST API, which may let the attacker violate security policy.<br>**REFERENCE: CVE-2016-6044** | http://www.ibm.com/support/docview.wss?uid=swg21995754 | A-IBM-TIVOL-280217/227 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| NA | 01-02-2017 | 4.4 | Tivoli Storage Manager Operations Center could allow a local user to take over a previously logged in user due to session expiration not being enforced. **REFERENCE: CVE-2016-6043** | http://www.ibm.com/support/docview.wss?uid=swg21995754 | A-IBM-TIVOL-280217/228 |
| Cross Site Request Forgery | 01-02-2017 | 6.8 | IBM Tivoli Storage Manager Operations Center is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. **REFERENCE: CVE-2016-6045** | http://www.ibm.com/support/docview.wss?uid=swg21995754 | A-IBM-TIVOL-280217/229 |
| Execute Code; Overflow | 01-02-2017 | 7.2 | The IBM Tivoli Storage Manager (IBM Spectrum Protect) AIX client is vulnerable to a buffer overflow when Journal-Based Backup is enabled. A local attacker could overflow a buffer and execute arbitrary code on the system or cause a system crash. **REFERENCE: CVE-2016-5985** | http://www.ibm.com/support/docview.wss?uid=swg21993695 | A-IBM-TIVOL-280217/230 |

***Tivoli Storage Manager Fastback***

IBM Spectrum Protect for Workstations (formerly IBM Tivoli Storage Manager FastBack for Workstations) is near real-time, continuous data protection software specifically designed for desktop and laptop computers.

| | | | | | |
|---|---|---|---|---|---|
| Execute Code | 08-02-2017 | 6.9 | IBM Tivoli Storage Manager FastBack installer could allow a remote attacker to execute arbitrary code on the system. By placing a specially-crafted DLL in | http://www.ibm.com/support/docview.wss?uid=swg21988908 | A-IBM-TIVOL-280217/231 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | the victim's path, an attacker could exploit this vulnerability when the installer is executed to run arbitrary code on the system with privileges of the victim.<br>**REFERENCE: CVE-2016-5934** | | |
| ***Tivoli Storage Manager For Space Management***<br>Use Tivoli Storage Manager for Space Management to move inactive or seldom-used files to server storage, freeing disk space for active data. | | | | | |
| Gain Information | 08-02-2017 | 1.9 | IBM Tivoli Storage Manager HSM for Windows displays the encrypted Tivoli Storage Manager password in application trace output if the password access option is prompt and the password is changed.<br>**REFERENCE: CVE-2016-5918** | http://www.ibm.com/support/docview.wss?uid=swg21988728 | A-IBM-TIVOL-280217/232 |
| ***Tivoli Storage Manager For Virtual Environments Data Protection For Vmware***<br>IBM Tivoli Storage Manager for Virtual Environments (referred to as Data Protection for VMware) provides a comprehensive solution for protecting VMs. | | | | | |
| Gain Information | 01-02-2017 | 4 | IBM Tivoli Storage Manager for Virtual Environments (VMware) could disclose the Windows domain credentials to a user with a high level of privileges.<br>**REFERENCE: CVE-2016-6034** | http://www.ibm.com/support/docview.wss?uid=swg21995544 | A-IBM-TIVOL-280217/233 |
| ***Tivoli Storage Manager; Tivoli Storage Manager For Virtual Environments Data Protection For Vmware***<br>IBM Spectrum Protect (Tivoli Storage Manager) is a data protection platform that gives enterprises a single point of control and administration for backup and recovery. | | | | | |
| NA | 01-02-2017 | 2.1 | IBM Tivoli Storage Manager undisclosed unencrypted login credentials to Vmware vCenter that could be obtained by a local user. | http://www.ibm.com/support/docview.wss?uid=swg21996198 | A-IBM-TIVOL-280217/234 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | **REFERENCE: CVE-2016-6110** |  |  |
| ***Tririga Application Platform***<br>IBM TRIRIGA Application Platform provides a single web-based set of design-time and runtime components. |  |  |  |  |  |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM TRIRIGA Application Platform is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-5980** | http://www.ibm.com/support/docview.wss?uid=swg21991992 | A-IBM-TRIRI-280217/235 |
| Cross Site Scripting | 01-02-2017 | 4.3 | IBM TRIRIGA Application Platform is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **REFERENCE: CVE-2016-6000** | http://www.ibm.com/support/docview.wss?uid=swg21991995 | A-IBM-TRIRI-280217/236 |
| ***Urbancode Deploy***<br>IBM UrbanCode Deploy is a tool for automating application deployments through your environments. |  |  |  |  |  |
| Execute Code; Gain Information | 01-02-2017 | 2.1 | IBM UrbanCode Deploy creates temporary files during step execution that could contain sensitive information including passwords that could be read by a local user. **REFERENCE: CVE-2016-2941** | http://www.ibm.com/support/docview.wss?uid=swg2C1000220 | A-IBM-URBAN-280217/237 |
| NA | 01-02-2017 | 4 | IBM UrbanCode Deploy could allow an authenticated user to | http://www.ibm.com/support/docview.wss?u | A-IBM-URBAN-280217/238 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | modify Ucd objects due to multiple REST endpoints not properly authorizing users editing UCD objects. This could affect the behavior of legitimately triggered processes. **REFERENCE: CVE-2016-0320** | id=swg2C1000222 | |
| NA | 01-02-2017 | 5 | IBM UrbanCode Deploy could allow a malicious user to access the Agent Relay ActiveMQ Broker JMX interface and run plugins on the agent. **REFERENCE: CVE-2016-9008** | http://www.ibm.com/support/docview.wss?uid=swg2C1000238 | A-IBM-URBAN-280217/239 |
| Gain Information | 01-02-2017 | 5 | IBM UrbanCode Deploy could allow an authenticated user with access to the REST endpoints to access API and CLI getResource secured role properties. **REFERENCE: CVE-2016-6068** | http://www.ibm.com/support/docview.wss?uid=swg2C1000229 | A-IBM-URBAN-280217/240 |
| NA | 01-02-2017 | 6 | IBM UrbanCode Deploy could allow an authenticated attacker with special permissions to craft a script on the server in a way that will cause processes to run on a remote UCD agent machine. **REFERENCE: CVE-2016-2942** | http://www.ibm.com/support/docview.wss?uid=swg2C1000218 | A-IBM-URBAN-280217/241 |
| Execute Code | 01-02-2017 | 10 | IBM UrbanCode Deploy could allow a user to execute code using a specially crafted file upload that would replace code on the server. This code could be executed on the UCD agent machines | http://www.ibm.com/support/docview.wss?uid=swg2C1000237 | A-IBM-URBAN-280217/242 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | that host customer's production applications.<br>**REFERENCE: CVE-2016-8938** | | |
| ***Websphere Application Server***<br>WebSphere Application Server (WAS) is a software product that performs the role of a web application server. | | | | | |
| Cross Site Scripting | 01-02-2017 | 3.5 | IBM WebSphere Application Server is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.<br>**REFERENCE: CVE-2016-8934** | http://www.ibm.com/support/docview.wss?uid=swg21995995 | A-IBM-WEBSP-280217/243 |
| Cross Site Scripting | 13-02-2017 | 3.5 | IBM WebSphere Application Server 7.0, 8.0, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1997743<br>**REFERENCE: CVE-2017-1121** | http://www.ibm.com/support/docview.wss?uid=swg21997743 | A-IBM-WEBSP-280217/244 |
| Denial of Service | 01-02-2017 | 7.8 | IBM WebSphere Application Server may be vulnerable to a denial of service, caused by allowing serialized objects from untrusted sources to run and cause the consumption of resources.<br>**REFERENCE: CVE-2016-** | http://www.ibm.com/support/docview.wss?uid=swg21993797 | A-IBM-WEBSP-280217/245 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | **8919** |  |  |
| ***Websphere Extreme Scale***<br>WebSphere Application Server (WAS) is a software product that performs the role of a web application server. |  |  |  |  |  |
| Gain Information | 08-02-2017 | 2.1 | IBM WebSphere eXtreme Scale and the WebSphere DataPower XC10 Appliance allow some sensitive data to linger in memory instead of being overwritten which could allow a local user with administrator privileges to obtain sensitive information.<br>**REFERENCE: CVE-2015-7418** | http://www.ibm.com/support/docview.wss?uid=swg21971657 | A-IBM-WEBSP-280217/246 |
| ***Websphere Message Broker***<br>IBM Integration Bus (formerly known as Web-Sphere Message Broker) is IBM's integration broker from the WebSphere product family that allows business information to flow between disparate applications across multiple hardware and software platforms. |  |  |  |  |  |
| Gain Information | 01-02-2017 | 5 | The WebAdmin context for WebSphere Message Broker allows directory listings which could disclose sensitive information to the attacker.<br>**REFERENCE: CVE-2016-6080** | http://www.ibm.com/support/docview.wss?uid=swg21995004 | A-IBM-WEBSP-280217/247 |
| ***Websphere Mq Jms***<br>WebSphere MQ classes for Java Message Service (WebSphere MQ classes for JMS) is the JMS provider that is supplied with WebSphere MQ. |  |  |  |  |  |
| Execute Code | 15-02-2017 | 7.5 | IBM Websphere MQ JMS 7.0.1, 7.1, 7.5, 8.0, and 9.0 client provides classes that deserialize objects from untrusted sources which could allow a malicious user to execute arbitrary Java code by adding vulnerable classes to the classpath. IBM Reference #: 1983457.<br>**REFERENCE: CVE-2016-** | http://www-01.ibm.com/support/docview.wss?uid=swg21983457 | A-IBM-WEBSP-280217/248 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | **0360** |  |  |
| **Imagemagick** |  |  |  |  |  |
| ***Imagemagick***<br>ImageMagick is a software suite to create, edit, compose, or convert bitmap images. |  |  |  |  |  |
| Denial of Service | 15-02-2017 | 4.3 | The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted file. NOTE: the vendor says "This is a Q64 issue and we do not support Q64."<br>**REFERENCE: CVE-2016-8678** | https://bugzilla.redhat.com/show_bug.cgi?id=1385694 | A-IMA-IMAGE-280217/249 |
| **Jappix Project** |  |  |  |  |  |
| ***Jappix***<br>Jappix is a full-featured XMPP web-client (Jappix Desktop, Jappix Mobile & Jappix Mini). |  |  |  |  |  |
| NA | 09-02-2017 | 4.3 | An incorrect implementation of "XEP-0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This CVE is for jappix 1.0.0 to 1.1.6.<br>**REFERENCE: CVE-2017-5602** | NA | A-JAP-JAPPI-280217/250 |
| **Jasper Project** |  |  |  |  |  |
| ***Jasper***<br>Jasper is an open source platform for developing always-on, voice-controlled applications. |  |  |  |  |  |
| Overflow | 15-02-2017 | 6.8 | Stack-based buffer overflow in the jpc_tsfb_getbands2 function in jpc_tsfb.c in JasPer before 1.900.30 allows remote attackers to | https://github.com/mdadams/jasper/commit/1abc2e5a401a4bf1d5ca4df91358ce5df111f49 | A-JAS-JASPE-280217/251 |

| | | | | | |
|---|---|---|---|---|---|
| | | | have unspecified impact via a crafted image.<br>**REFERENCE: CVE-2016-9560** | 5 | |
| **Jenkins** | | | | | |
| ***Extra Columns Plugin***<br>NA | | | | | |
| Cross Site Scripting | 09-02-2017 | 4.3 | Cross-site scripting (XSS) vulnerability in the Extra Columns plugin before 1.17 in Jenkins allows remote attackers to inject arbitrary web script or HTML by leveraging failure to filter tool tips through the configured markup formatter.<br>**REFERENCE: CVE-2016-3101** | https://wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2016-04-11 | A-JEN-EXTRA-280217/252 |
| ***Image Gallery Plugin***<br>Image Gallery is the best plugin among WordPress gallery plugins. | | | | | |
| Directory Traversal | 09-02-2017 | 5 | Directory traversal vulnerability in the Image Gallery plugin before 1.4 in Jenkins allows remote attackers to list arbitrary directories and read arbitrary files via unspecified form fields.<br>**REFERENCE: CVE-2016-4987** | https://wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2016-06-20 | A-JEN-IMAGE-280217/253 |
| ***Tap Plugin***<br>Tom's Audio Processing plugins for audio engineering on the Linux platform. | | | | | |
| Directory Traversal | 09-02-2017 | 5 | Directory traversal vulnerability in the TAP plugin before 1.25 in Jenkins allows remote attackers to read arbitrary files via an unspecified parameter.<br>**REFERENCE: CVE-2016-4986** | https://wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2016-06-20 | A-JEN-TAP P-280217/254 |
| **Jenkins-ci** | | | | | |
| ***Build Failure Analyzer***<br>The Build Failure Analyzer plugin lets you set regular expressions for categorizing current and future | | | | | |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| builds. | | | | | |
| Cross Site Scripting | 09-02-2017 | 4.3 | Cross-site scripting (XSS) vulnerability in the Build Failure Analyzer plugin before 1.16.0 in Jenkins allows remote attackers to inject arbitrary web script or HTML via an unspecified parameter.<br>**REFERENCE: CVE-2016-4988** | https://wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2016-06-20 | A-JEN-BUILD-280217/255 |
| **Jitsi** | | | | | |
| ***Jitsi***<br>Jitsi - Open Source Video Calls and Chat. Secure video calls, conferencing, chat, desktop sharing, file transfer, support for your favorite OS, and IM network. | | | | | |
| NA | 09-02-2017 | 4.3 | An incorrect implementation of "XEP-0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This CVE is for Jitsi 2.5.5061 - 2.9.5544.<br>**REFERENCE: CVE-2017-5603** | NA | A-JIT-JITSI-280217/256 |
| **Kabona Ab** | | | | | |
| ***Webdatorcentral***<br>'WDC' (WebDatorCentral), a web-based unit for monitoring and operation of systems for heating, cooling and ventilation. | | | | | |
| Cross Site Scripting | 13-02-2017 | 4.3 | An issue was discovered in Kabona AB WebDatorCentral (WDC) application prior to Version 3.4.0. The web server URL inputs are not sanitized correctly, which may allow cross-site scripting vulnerabilities.<br>**REFERENCE: CVE-2016-8356** | NA | A-KAB-WEBDA-280217/257 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| NA | 13-02-2017 | 5.8 | An issue was discovered in Kabona AB WebDatorCentral (WDC) application prior to Version 3.4.0. This non-validated redirect/non-validated forward (OPEN REDIRECT) allows chaining with authenticated vulnerabilities. **REFERENCE: CVE-2016-8376** | NA | A-KAB-WEBDA-280217/258 |
| **Knot Dns Project** | | | | | |
| ***Knot Dns***<br>Knot DNS is an open-source server program for the Domain Name System. | | | | | |
| Denial of Service | 09-02-2017 | 5 | Knot DNS before 2.3.0 allows remote DNS servers to cause a denial of service (memory exhaustion and slave server crash) via a large zone transfer for (1) DDNS, (2) AXFR, or (3) IXFR. **REFERENCE: CVE-2016-6171** | https://gitlab.labs.nic.cz/labs/knot/issues/464 | A-KNO-KNOT -280217/259 |
| **Lepton Project** | | | | | |
| ***Lepton***<br>Lepton is a tool and file format for losslessly compressing JPEGs by an average of 22%. | | | | | |
| Denial of Service | 02-02-2017 | 4.3 | The write_ujpg function in lepton/jpgcoder.cc in Dropbox lepton 1.0 allows remote attackers to cause denial of service (out-of-bounds read) via a crafted jpeg file. **REFERENCE: CVE-2016-6238** | https://github.com/dropbox/lepton/issues/26 | A-LEP-LEPTO-280217/260 |
| Denial of Service | 02-02-2017 | 4.3 | The build_huffcodes function in lepton/jpgcoder.cc in Dropbox lepton 1.0 allows remote attackers to cause denial of service (out-of- | https://github.com/dropbox/lepton/issues/26 | A-LEP-LEPTO-280217/261 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | bounds write) via a crafted jpeg file.<br>**REFERENCE: CVE-2016-6237** | | |
| Denial of Service | 02-02-2017 | 4.3 | The setup_imginfo_jpg function in lepton/jpgcoder.cc in Dropbox lepton 1.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted jpeg file.<br>**REFERENCE: CVE-2016-6236** | https://github.com/dropbox/lepton/issues/26 | A-LEP-LEPTO-280217/262 |
| Denial of Service | 02-02-2017 | 4.3 | The setup_imginfo_jpg function in lepton/jpgcoder.cc in Dropbox lepton 1.0 allows remote attackers to cause a denial of service (segmentation fault) via a crafted jpeg file.<br>**REFERENCE: CVE-2016-6235** | https://github.com/dropbox/lepton/issues/26 | A-LEP-LEPTO-280217/263 |
| Denial of Service | 02-02-2017 | 4.3 | The process_file function in lepton/jpgcoder.cc in Dropbox lepton 1.0 allows remote attackers to cause a denial of service (crash) via a crafted jpeg file.<br>**REFERENCE: CVE-2016-6234** | https://github.com/dropbox/lepton/issues/26 | A-LEP-LEPTO-280217/264 |
| **Libav** | | | | | |
| ***Libav***<br>Libav is a free software project, forked from FFmpeg in 2011, that produces libraries and programs for handling multimedia data. | | | | | |
| Denial of Service | 15-02-2017 | 4.3 | The get_vlc2 function in get_bits.h in Libav 11.9 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted mp3 file. NOTE: this issue exists due to an incomplete fix for | NA | A-LIB-LIBAV-280217/265 |

| CV Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | REFERENCE: CVE-2016-8675.<br>**REFERENCE: CVE-2016-8676** | | |
| Denial of Service | 15-02-2017 | 4.3 | The get_vlc2 function in get_bits.h in Libav before 11.9 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted mp3 file, possibly related to startcode sequences during m4v detection.<br>**REFERENCE: CVE-2016-8675** | https://github.com/libav/libav/commit/e5b019725f53b79159931d3a7317107cbbfd0860 | A-LIB-LIBAV-280217/266 |
| Denial of Service | 15-02-2017 | 4.3 | The sbr_make_f_master function in aacsbr.c in Libav 11.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted mp3 file.<br>**REFERENCE: CVE-2016-7499** | https://git.libav.org/?p=libav.git;a=blobdiff;f=libavcodec/aacsbr.c;h=7d156e525b40b197c38db17acf16730845b91e56;hp=dbfb1677813ce6c531e4362d0be7ccf9fdfdd28e;hb=a50a5ff29ec5a8243499769e2bb9b5509ce9fd52;hpb=f55e3ff5891daf3d538b4d9176371960200d68fa | A-LIB-LIBAV-280217/267 |
| Denial of Service | 15-02-2017 | 4.3 | The ff_put_pixels8_xy2_mmx function in rnd_template.c in Libav 11.7 allows remote attackers to cause a denial of service (invalid memory access and crash) via a crafted mp3 file. NOTE: this issue was originally reported as involving a NULL pointer | NA | A-LIB-LIBAV-280217/268 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | dereference.<br>**REFERENCE: CVE-2016-7477** | | |
| Denial of Service; Overflow | 15-02-2017 | 4.3 | Stack-based buffer overflow in the aac_sync function in aac_parser.c in Libav before 11.5 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.<br>**REFERENCE: CVE-2016-7393** | https://git.libav.org/?p=libav.git;a=commit;h=fb1473080223a634b8ac2cca48a632d037a0a69d | A-LIB-LIBAV-280217/269 |
| Denial of Service; Overflow | 15-02-2017 | 4.3 | Heap-based buffer overflow in the ff_audio_resample function in resample.c in libav before 11.4 allows remote attackers to cause a denial of service (crash) via vectors related to buffer resizing.<br>**REFERENCE: CVE-2016-6832** | https://git.libav.org/?p=libav.git;a=commit;h=0ac8ff618c5e6d878c547a8877e714ed728950ce | A-LIB-LIBAV-280217/270 |
| **Libavformat Project** | | | | | |
| ***Libavformat***<br>Libavformat (lavf) is a library for dealing with various media container formats. | | | | | |
| Denial of Service | 03-02-2017 | 4.3 | The avcodec_decode_audio4 function in libavcodec in libavformat 57.34.103, as used in MPlayer, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mp3 file.<br>**REFERENCE: CVE-2016-5115** | https://trac.mplayerhq.hu/ticket/2298 | A-LIB-LIBAV-280217/271 |
| Denial of Service; Overflow | 03-02-2017 | 4.3 | Integer overflow in the demuxer function in libmpdemux/demux_gif.c in Mplayer allows remote attackers to cause a denial of service (crash) via large dimensions in a gif file. | https://trac.mplayerhq.hu/ticket/2295 | A-LIB-LIBAV-280217/272 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | **REFERENCE: CVE-2016-4352** | | |
| **Libdwarf Project** | | | | | |
| ***Libdwarf***<br>Libdwarf is a C library intended to simplify reading (and writing) applications using DWARF2, DWARF3. | | | | | |
| Denial of Service | 13-02-2017 | 4.3 | libdwarf 20151114 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a debug_abbrev section marked NOBITS in an ELF file.<br>**REFERENCE: CVE-2015-8750** | https://github.com/tomhughes/libdwarf/commit/11750a2838e52953013e3114ef27b3c7b1780697 | A-LIB-LIBDW-280217/273 |
| Denial of Service | 15-02-2017 | 4.3 | The _dwarf_get_abbrev_for_code function in dwarf_util.c in libdwarf 20161001 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) by calling the dwarfdump command on a crafted file.<br>**REFERENCE: CVE-2016-8681** | https://bugzilla.redhat.com/show_bug.cgi?id=1385690 | A-LIB-LIBDW-280217/274 |
| Denial of Service | 15-02-2017 | 4.3 | The _dwarf_get_abbrev_for_code function in dwarf_util.c in libdwarf 20161001 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) by calling the dwarfdump command on a crafted file.<br>**REFERENCE: CVE-2016-8680** | https://sourceforge.net/p/libdwarf/code/ci/268c1f18d1d28612af3b72d7c670076b1b88e51c/tree/libdwarf/dwarf_util.c?diff=0b28b923c3bd9827d1d904feed2abadde4fa5de2 | A-LIB-LIBDW-280217/275 |
| Denial of Service | 15-02-2017 | 4.3 | The _dwarf_get_size_of_val function in libdwarf/dwarf_util.c in Libdwarf before 20161124 allows remote | https://bugzilla.redhat.com/show_bug.cgi?id=1385689 | A-LIB-LIBDW-280217/276 |

| | | | | | |
|---|---|---|---|---|---|
| | | | attackers to cause a denial of service (out-of-bounds read) by calling the dwarfdump command on a crafted file.<br>**REFERENCE: CVE-2016-8679** | | |
| **Libtiff** | | | | | |
| ***Libtiff***<br>Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files. | | | | | |
| Denial of Service; Overflow | 06-02-2017 | 4.3 | Buffer overflow in the readgifimage function in gif2tiff.c in the gif2tiff tool in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (segmentation fault) via a crafted gif file.<br>**REFERENCE: CVE-2016-5102** | http://bugzilla.maptools.org/show_bug.cgi?id=2552 | A-LIB-LIBTI-280217/277 |
| **Libtorrent** | | | | | |
| ***Libtorrent***<br>libtorrent is a feature complete C++ bittorrent implementation focusing on efficiency and scalability. | | | | | |
| Denial of Service | 07-02-2017 | 5 | The construct function in puff.cpp in Libtorrent 1.1.0 allows remote torrent trackers to cause a denial of service (segmentation fault and crash) via a crafted GZIP response.<br>**REFERENCE: CVE-2016-7164** | https://github.com/arvidn/libtorrent/pull/1022 | A-LIB-LIBTO-280217/278 |
| **Libxpm Project** | | | | | |
| ***Libxpm***<br>LibXpm provides support and common operation for the XPM pixmap format, which is commonly used in legacy X applications. | | | | | |
| Denial of Service; Execute Code; Overflow | 01-02-2017 | 7.5 | Multiple integer overflows in libXpm before 3.5.12, when a program requests parsing XPM extensions on a 64-bit platform, allow remote attackers to cause a denial of service (out-of-bounds write) or execute | https://cgit.freedesktop.org/xorg/lib/libXpm/commit/?id=d1167418f0fd02a27f617ec5afd6db053afbe185 | A-LIB-LIBXP-280217/279 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | arbitrary code via (1) the number of extensions or (2) their concatenated length in a crafted XPM file, which triggers a heap-based buffer overflow.<br>**REFERENCE: CVE-2016-10164** |  |  |
| **Lynxspring** |  |  |  |  |  |
| ***Jenesys Bas Bridge***<br>The JENEsys Building Operating System is streamlining all areas building operation, maintenance management, energy management, and facility usage and technology management, and addresses these challenges by delivering a proven solution for interoperability and efficiency whether it is small or large institution or campus environment. |  |  |  |  |  |
| NA | 13-02-2017 | 5 | An issue was discovered in Lynxspring JENEsys BAS Bridge versions 1.1.8 and older. The application's database lacks sufficient safeguards for protecting credentials.<br>**REFERENCE: CVE-2016-8378** | NA | A-LYN-JENES-280217/280 |
| NA | 13-02-2017 | 5.5 | An issue was discovered in Lynxspring JENEsys BAS Bridge versions 1.1.8 and older. A user with read-only access can send commands to the software and the application will accept those commands. This would allow an attacker with read-only access to make changes within the application.<br>**REFERENCE: CVE-2016-8357** | NA | A-LYN-JENES-280217/281 |
| Cross Site Request Forgery | 13-02-2017 | 6.8 | An issue was discovered in Lynxspring JENEsys BAS Bridge versions 1.1.8 and older. The application does not sufficiently verify if a request was intentionally provided by the user who submitted | NA | A-LYN-JENES-280217/282 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | the request (CROSS-SITE REQUEST FORGERY). **REFERENCE: CVE-2016-8369** | | |
| NA | 13-02-2017 | 7.5 | An issue was discovered in Lynxspring JENEsys BAS Bridge versions 1.1.8 and older. The application uses a hard-coded username with no password allowing an attacker into the system without authentication. **REFERENCE: CVE-2016-8361** | NA | A-LYN-JENES-280217/283 |
| **Mariadb;Oracle** | | | | | |
| ***Mariadb/Mysql***<br>MariaDB is a community-developed fork of the MySQL relational database management system intended to remain free under the GNU GPL/ MySQL is an open-source relational database management system (RDBMS). | | | | | |
| NA | 11-02-2017 | 5 | Crash in libmysqlclient.so in Oracle MySQL before 5.6.21 and 5.7.x before 5.7.5 and MariaDB through 5.5.54, 10.0.x through 10.0.29, 10.1.x through 10.1.21, and 10.2.x through 10.2.3. **REFERENCE: CVE-2017-3302** | http://www.openwall.com/lists/oss-security/2017/02/11/11 | A-MAR-MARIA-280217/284 |
| **Mcabber** | | | | | |
| ***Mcabber***<br>MCabber is a free software client for the instant messaging protocol XMPP with a text user interface based on ncurses. | | | | | |
| NA | 09-02-2017 | 4.3 | An incorrect implementation of "XEP-0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This | NA | A-MCA-MCABB-280217/285 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | CVE is for mcabber 1.0.0 - 1.0.4.<br>**REFERENCE: CVE-2017-5604** |  |  |
| **Mcafee** |  |  |  |  |  |
| ***Epolicy Orchestrator***<br>McAfee ePolicy Orchestrator (McAfee ePO) is the most advanced, extensible, and scalable centralized security management software in the industry. |  |  |  |  |  |
| Cross Site Scripting; Bypass | 13-02-2017 | 3.5 | Cross-site scripting (XSS) vulnerability in the Web user interface (UI) in Intel Security ePO 5.1.3, 5.1.2, 5.1.1, and 5.1.0 allows authenticated users to inject malicious Java scripts via bypassing input validation.<br>**REFERENCE: CVE-2017-3902** | https://kc.mcafee.com/corporate/index?page=content&id=SB10184 | A-MCA-EPOLI-280217/286 |
| **Modified** |  |  |  |  |  |
| ***Ecommerce Shopsoftware***<br>NA |  |  |  |  |  |
| Execute Code; SQL Injection | 15-02-2017 | 7.5 | Multiple SQL injection vulnerabilities in modified eCommerce Shopsoftware 2.0.0.0 revision 9678, when the easybill-module is not installed, allow remote attackers to execute arbitrary SQL commands via the (1) orders_status or (2) customers_status parameter to api/easybill/easybillcsv.php.<br>**REFERENCE: CVE-2016-3694** | NA | A-MOD-ECOMM-280217/287 |
| **Movim** |  |  |  |  |  |
| ***Movim***<br>MOVIM is a distributed social network built on top of XMPP, a popular open standards communication protocol. |  |  |  |  |  |
| NA | 09-02-2017 | 4.3 | An incorrect implementation of "XEP-0280: Message Carbons" | NA | A-MOV-MOVIM-280217/288 |

| CV Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This CVE is for Movim 0.8 - 0.10.<br>**REFERENCE: CVE-2017-5605** | | |
| **Moxa** | | | | | |
| ***Dacenter***<br>DA-Center provides a standard OPC interface that interacts with Moxa Active OPC Server for real-time data collection. | | | | | |
| NA | 13-02-2017 | 4.6 | An issue was discovered in Moxa DACenter Versions 1.4 and older. The application may suffer from an unquoted search path issue.<br>**REFERENCE: CVE-2016-9356** | NA | A-MOX-DACEN-280217/289 |
| NA | 13-02-2017 | 7.1 | An issue was discovered in Moxa DACenter Versions 1.4 and older. A specially crafted project file may cause the program to crash because of Uncontrolled Resource Consumption.<br>**REFERENCE: CVE-2016-9354** | NA | A-MOX-DACEN-280217/290 |
| ***Softcms***<br>SoftCMS is a powerful central management software solution that manages large scale CCTV installations in a single interface. | | | | | |
| SQL Injection | 13-02-2017 | 6.5 | An issue was discovered in Moxa SoftCMS versions prior to Version 1.6. The SoftCMS Application does not properly sanitize input that may allow a remote attacker access to SoftCMS with administrator's | NA | A-MOX-SOFTC-280217/291 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | privilege through specially crafted input (SQL INJECTION).<br>**REFERENCE: CVE-2016-9333** | | |
| Denial of Service; Execute Code | 13-02-2017 | 6.8 | An issue was discovered in Moxa SoftCMS versions prior to Version 1.6. A specially crafted URL request sent to the SoftCMS ASP Webserver can cause a double free condition on the server allowing an attacker to modify memory locations and possibly cause a denial of service or the execution of arbitrary code.<br>**REFERENCE: CVE-2016-8360** | NA | A-MOX-SOFTC-280217/292 |
| NA | 13-02-2017 | 7.8 | An issue was discovered in Moxa SoftCMS versions prior to Version 1.6. Moxa SoftCMS Webserver does not properly validate input. An attacker could provide unexpected values and cause the program to crash or excessive consumption of resources could result in a denial-of-service condition.<br>**REFERENCE: CVE-2016-9332** | NA | A-MOX-SOFTC-280217/293 |
| **Msweet** | | | | | |
| ***Mini-xml***<br>Mini-XML is a small XML library that you can use to read and write XML and XML-like data files in your application without requiring large non-standard libraries. | | | | | |
| Denial of Service | 03-02-2017 | 7.1 | The mxml_write_node function in mxml-file.c in mxml 2.9, 2.7, and possibly earlier allows remote attackers to cause a denial of service (stack | https://bugzilla.redhat.com/show_bug.cgi?id=1334648 | A-MSW-MINI--280217/294 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | consumption) via crafted xml file. **REFERENCE: CVE-2016-4571** | | |
| Denial of Service | 03-02-2017 | 7.1 | The mxmlDelete function in mxml-node.c in mxml 2.9, 2.7, and possibly earlier allows remote attackers to cause a denial of service (stack consumption) via crafted xml file. **REFERENCE: CVE-2016-4570** | https://bugzilla.redhat.com/show_bug.cgi?id=1334648 | A-MSW-MINI--280217/295 |
| **Nagios** | | | | | |
| ***Nagios***<br>Nagios provides enterprise-class Open Source IT monitoring, network monitoring, server and applications monitoring. | | | | | |
| Gain Privileges | 15-02-2017 | 7.2 | Nagios 4.2.4 and earlier allows local users to gain root privileges via a hard link attack on the Nagios init script file, related to CVE-2016-8641. **REFERENCE: CVE-2016-10089** | NA | A-NAG-NAGIO-280217/296 |
| **Netapp** | | | | | |
| ***Clustered Data Ontap***<br>Clustered Data ONTAP provides up to 24 storage controllers or nodes managed as a single logical pool so your operations scale more easily. | | | | | |
| Gain Information | 07-02-2017 | 5 | NetApp Clustered Data ONTAP before 8.3.2P7 allows remote attackers to obtain SMB share information via unspecified vectors. **REFERENCE: CVE-2016-4341** | https://kb.netapp.com/support/s/article/NTAP-20161028-0001 | A-NET-CLUST-280217/297 |
| ***Oncommand Insight***<br>OnCommand Insight helps large enterprise-customers manage capacity, performance, forecasting, and multi-tenant billing in traditional and cloud environments. | | | | | |
| NA | 02-02-2017 | 7.5 | The Data Warehouse component in NetApp OnCommand Insight before 7.2.3 allows remote | https://kb.netapp.com/support/s/article/NTAP-20170131- | A-NET-ONCOM-280217/298 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | attackers to obtain administrative access by leveraging a default privileged account.<br>**REFERENCE: CVE-2017-5600** | 0001 | |
| ***Oncommand System Manager***<br>OnCommand System Manager provides fast, simple configuration and management for NetApp FAS storage systems. | | | | | |
| Execute Code | 07-02-2017 | 4.4 | Multiple functions in NetApp OnCommand System Manager before 8.3.2 do not properly escape special characters, which allows remote authenticated users to execute arbitrary API calls via unspecified vectors.<br>**REFERENCE: CVE-2016-3063** | https://kb.netapp.com/support/s/article/Reference: CVE-2016-3063-zapi-injection-vulnerability-in-oncommand-system-manager | A-NET-ONCOM-280217/299 |
| ***Oncommand Unified Manager For Clustered Data Ontap***<br>OnCommand Unified Manager monitors and alerts on the health of your NetApp storage running onclustered Data ONTAP. | | | | | |
| Execute Code | 07-02-2017 | 7.5 | NetApp OnCommand Unified Manager for Clustered Data ONTAP 6.3 through 6.4P1 contain a default privileged account, which allows remote attackers to execute arbitrary code via unspecified vectors.<br>**REFERENCE: CVE-2016-6667** | https://kb.netapp.com/support/s/article/NTAP-20161017-0002 | A-NET-ONCOM-280217/300 |
| ***Oncommand Workflow Automation***<br>The NetApp OnCommand Workflow Automation solution improves productivity in your organization by automating storage-management processes. | | | | | |
| Bypass | 07-02-2017 | 9.3 | NetApp OnCommand Workflow Automation before 3.1P2 allows remote attackers to bypass authentication via unspecified vectors.<br>**REFERENCE: CVE-2016-1894** | https://kb.netapp.com/support/s/article/Reference: CVE-2016-1894-authentication-bypass-vulnerability- | A-NET-ONCOM-280217/301 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  |  | in-oncommand-workflow-automation |  |
| ***Snap Creator Framework***<br>The OS-independent NetApp Snap Creator, which integrates with NetApp unified data protection technologies and delivers application-consistent data. |  |  |  |  |  |
| Cross Site Request Forgery | 07-02-2017 | 6.8 | Cross-site request forgery (CSRF) vulnerability in NetApp Snap Creator Framework before 4.3.0P1 allows remote attackers to hijack the authentication of users for requests that have unspecified impact via unknown vectors. **REFERENCE: CVE-2016-5372** | https://kb.netapp.com/support/s/article/Reference: CVE-2016-5372-cross-site-request-forgery-vulnerability-in-snap-creator-framework | A-NET-SNAP -280217/302 |
| ***Snapcenter Server***<br>NetApp SnapCenter Software is a unified, scalable platform for application-consistent data protection. SnapCenter provides centralized control and oversight, while delegating the ability for users to manage application-specific backup, restore, and clone jobs. |  |  |  |  |  |
| Bypass | 07-02-2017 | 7.5 | NetApp SnapCenter Server 1.0 and 1.0P1 allows remote attackers to partially bypass authentication and then list and delete backups via unspecified vectors. **REFERENCE: CVE-2016-1502** | https://kb.netapp.com/support/s/article/authentication-bypass-vulnerability-in-snapcenter-server-1-0-1-0p1 | A-NET-SNAPC-280217/303 |
| ***Snapdrive***<br>NetApp SnapDrive for Microsoft Windows improves IT efficiency and automates data storage in physical and virtual environments. |  |  |  |  |  |
| Gain Information | 07-02-2017 | 5 | NetApp SnapDrive for Windows before 7.0.2P4, 7.0.3, and 7.1 before 7.1.3P1 allows remote attackers to obtain sensitive information via unspecified vectors. **REFERENCE: CVE-2015-8544** | https://kb.netapp.com/support/s/article/Reference: CVE-2015-8544-sensitive-information-disclosure-in-snapdrive-for-windows | A-NET-SNAPD-280217/304 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| ***Virtual Storage Console For Vmware Vsphere***<br>NetApp Virtual Storage Console for Vmware vSphere improves efficiency and reduces cost and complexity in a VMware virtual infrastructure. | | | | | |
| NA | 07-02-2017 | 6.8 | NetApp Virtual Storage Console for VMware vSphere before 6.2.1 uses a non-unique certificate, which allows remote attackers to conduct man-in-the-middle attacks via unspecified vectors.<br>**REFERENCE: CVE-2016-5711** | https://kb.netapp.com/support/s/article/NTAP-20161108-0001 | A-NET-VIRTU-280217/305 |
| **Nitro Software** | | | | | |
| ***Nitro Pro***<br>With Nitro Pro you can open, review, covert and create PDF files. | | | | | |
| Memory Corruption | 10-02-2017 | 6.8 | A remote out of bound write / memory corruption vulnerability exists in the PDF parsing functionality of Nitro Pro 10.5.9.9. A specially crafted PDF file can cause a vulnerability resulting in potential memory corruption. An attacker can send the victim a specific PDF file to trigger this vulnerability.<br>**REFERENCE: CVE-2016-8713** | http://www.talosintelligence.com/reports/TALOS-2016-0226/ | A-NIT-NITRO-280217/306 |
| Execute Code | 10-02-2017 | 6.8 | A potential remote code execution vulnerability exists in the PDF parsing functionality of Nitro Pro 10. A specially crafted PDF file can cause a vulnerability resulting in potential code execution. An attacker can send the victim a specific PDF file to trigger this vulnerability.<br>**REFERENCE: CVE-2016-8711** | http://www.talosintelligence.com/reports/TALOS-2016-0224/ | A-NIT-NITRO-280217/307 |
| Overflow; | 10-02-2017 | 6.8 | A remote out of bound | http://www.tal | A-NIT- |

| CV Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Memory Corruption | | | write / memory corruption vulnerability exists in the PDF parsing functionality of Nitro Pro 10. A specially crafted PDF file can cause a vulnerability resulting in potential memory corruption. An attacker can send the victim a specific PDF file to trigger this vulnerability.<br>**REFERENCE: CVE-2016-8709** | osintelligence.com/reports/TALOS-2016-0218/ | NITRO-280217/308 |
| **Nlnetlabs** | | | | | |
| ***NSD***<br>In Internet computing, NSD (for "name server daemon") is an open-source Domain Name System (DNS) server. | | | | | |
| Denial of Service | 09-02-2017 | 7.8 | NSD before 4.1.11 allows remote DNS master servers to cause a denial of service (/tmp disk consumption and slave server crash) via a zone transfer with unlimited data.<br>**REFERENCE: CVE-2016-6173** | http://www.nlnetlabs.nl/svn/nsd/tags/NSD_4_1_11_REL/doc/RELNOTES | A-NLN-NSD-280217/309 |
| **Nvidia** | | | | | |
| ***Gpu Driver***<br>GPU-accelerated computing is the use of a graphics processing unit (GPU) together with a CPU to accelerate deep learning, analytics, and engineering applications. Pioneered in 2007 by NVIDIA, GPU accelerators now power energy-efficient data centers in government labs, universities, enterprises, and small-and-medium businesses around the world. They play a huge role in accelerating applications in platforms ranging from artificial intelligence to cars, drones, and robots. | | | | | |
| Denial of Service | 15-02-2017 | 4.9 | All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer handler where improper handling of values may cause a denial of service on the system.<br>**REFERENCE: CVE-2017-0320** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPUD-280217/310 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Denial of Service | 15-02-2017 | 4.9 | All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer handler where improper handling of values may cause a denial of service on the system.<br>**REFERENCE: CVE-2017-0319** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPU D-280217/311 |
| Denial of Service | 15-02-2017 | 4.9 | All versions of NVIDIA Linux GPU Display Driver contain a vulnerability in the kernel mode layer handler where improper validation of an input parameter may cause a denial of service on the system.<br>**REFERENCE: CVE-2017-0318** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPU D-280217/312 |
| Denial of Service | 15-02-2017 | 4.9 | All versions of NVIDIA GPU Display Driver contain a vulnerability in the kernel mode layer handler where improper access controls allowing unprivileged user to cause a denial of service.<br>**REFERENCE: CVE-2017-0310** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPU D-280217/313 |
| Execute Code | 15-02-2017 | 6.9 | All versions of NVIDIA GPU and GeForce Experience installer contain a vulnerability where it fails to set proper permissions on the package extraction path thus allowing a non-privileged user to tamper with the extracted files, potentially leading to escalation of privileges via code execution.<br>**REFERENCE: CVE-2017-** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPU D-280217/314 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | **0317** | | |
| Denial of Service; Overflow | 15-02-2017 | 7.2 | All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where the size of an input buffer is not validated, leading to denial of service or potential escalation of privileges.<br>**REFERENCE: CVE-2017-0324** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPUD-280217/315 |
| Denial of Service | 15-02-2017 | 7.2 | All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer handler where a NULL pointer dereference caused by invalid user input may lead to denial of service or potential escalation of privileges.<br>**REFERENCE: CVE-2017-0323** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPUD-280217/316 |
| Denial of Service | 15-02-2017 | 7.2 | All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler where a value passed from a user to the driver is not correctly validated and used as the index to an array, leading to denial of service or potential escalation of privileges.<br>**REFERENCE: CVE-2017-0322** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPUD-280217/317 |
| Denial of Service | 15-02-2017 | 7.2 | All versions of NVIDIA GPU Display Driver | http://nvidia.custhelp.com/app | A-NVI-GPUD- |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | contain a vulnerability in the kernel mode layer handler where a NULL pointer dereference caused by invalid user input may lead to denial of service or potential escalation of privileges. **REFERENCE: CVE-2017-0321** | /answers/detail/a_id/4398 | 280217/318 |
| Denial of Service | 15-02-2017 | 7.2 | All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where an attempt to access an invalid object pointer may lead to denial of service or potential escalation of privileges. **REFERENCE: CVE-2017-0315** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPU D-280217/319 |
| Denial of Service; Overflow | 15-02-2017 | 7.2 | All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) implementation of the SubmitCommandVirtual DDI (DxgkDdiSubmitCommandVirtual) where untrusted input is used to reference memory outside of the intended boundary of the buffer leading to denial of service or escalation of privileges. **REFERENCE: CVE-2017-0314** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPU D-280217/320 |
| Denial of Service; | 15-02-2017 | 7.2 | All versions of NVIDIA Windows GPU Display | http://nvidia.custhelp.com/app | A-NVI-GPU D- |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Overflow | | | Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) implementation of the SubmitCommandVirtual DDI (DxgkDdiSubmitCommandVirtual) where untrusted input is used to reference memory outside of the intended boundary of the buffer leading to denial of service or escalation of privileges.<br>**REFERENCE: CVE-2017-0313** | /answers/detail/a_id/4398 | 280217/321 |
| Denial of Service | 15-02-2017 | 7.2 | All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscapeID 0x100008b where user provided input is used as the limit for a loop may lead to denial of service or potential escalation of privileges<br>**REFERENCE: CVE-2017-0312** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPUD-280217/322 |
| Denial of Service | 15-02-2017 | 7.2 | NVIDIA GPU Display Driver R378 contains a vulnerability in the kernel mode layer handler where improper access control may lead to denial of service or possible escalation of privileges.<br>**REFERENCE: CVE-2017-0311** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPUD-280217/323 |
| Denial of Service; Overflow | 15-02-2017 | 7.2 | All versions of NVIDIA GPU Display Driver contain a vulnerability in | http://nvidia.custhelp.com/app/answers/detai | A-NVI-GPUD-280217/324 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | the kernel mode layer handler where multiple integer overflows may cause improper memory allocation leading to a denial of service or potential escalation of privileges.<br>**REFERENCE: CVE-2017-0309** | l/a_id/4398 |  |
| Denial of Service; Overflow | 15-02-2017 | 7.2 | All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where untrusted input is used for buffer size calculation leading to denial of service or escalation of privileges.<br>**REFERENCE: CVE-2017-0308** | http://nvidia.custhelp.com/app/answers/detail/a_id/4398 | A-NVI-GPUD-280217/325 |
| **Omnimetrix** |  |  |  |  |  |
| ***Omniview***<br>OmniMetrix is the leader and pioneer in M2M wireless remote monitoring and control for pipelines, stand-by generators and other critical equipment. |  |  |  |  |  |
| NA | 13-02-2017 | 5 | An issue was discovered in OmniMetrix OmniView, Version 1.2. Insufficient password requirements for the OmniView web application may allow an attacker to gain access by brute forcing account passwords.<br>**REFERENCE: CVE-2016-5801** | NA | A-OMN-OMNIV-280217/326 |
| Gain Information | 13-02-2017 | 5 | An issue was discovered in OmniMetrix OmniView, Version 1.2. The OmniView web application transmits credentials with the HTTP protocol, which could be | NA | A-OMN-OMNIV-280217/327 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | sniffed by an attacker that may result in the compromise of account credentials.<br>**REFERENCE: CVE-2016-5786** | | |
| **Openafs** | | | | | |
| ***Openafs***<br>Coordination and distribution of OpenAFS, an opensource implementation of the Andrew File System, including client and server software. | | | | | |
| Gain Information | 06-02-2017 | 5 | OpenAFS 1.6.19 and earlier allows remote attackers to obtain sensitive directory information via vectors involving the (1) client cache partition, (2) fileserver vice partition, or (3) certain RPC responses.<br>**REFERENCE: CVE-2016-9772** | https://www.openafs.org/pages/security/OPENAFS-SA-2016-003.txt | A-OPE-OPENA-280217/328 |
| **Openjpeg** | | | | | |
| ***Openjpeg***<br>OpenJPEG is an open-source JPEG 2000 codec written in C language. | | | | | |
| Denial of Service | 03-02-2017 | 4.3 | The sycc422_t_rgb function in common/color.c in OpenJPEG before 2.1.1 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted jpeg2000 file.<br>**REFERENCE: CVE-2016-3183** | https://bugzilla.redhat.com/show_bug.cgi?id=1317821 | A-OPE-OPENJ-280217/329 |
| **Plone** | | | | | |
| ***Plone***<br>Plone is a free and open source content management system built on top of the Zope application server. | | | | | |
| Cross Site Scripting | 04-02-2017 | 4.3 | Cross-site scripting (XSS) vulnerability in the manage_findResult component in the search feature in Zope ZMI in Plone before 4.3.12 and 5.x before 5.0.7 allows | NA | A-PLO-PLONE-280217/330 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | remote attackers to inject arbitrary web script or HTML via vectors involving double quotes, as demonstrated by the obj_ids:tokens parameter. NOTE: this vulnerability exists because of an incomplete fix for REFERENCE: CVE-2016-7140.<br>**REFERENCE: CVE-2016-7147** | | |
| **Profanity** | | | | | |
| ***Profanity***<br>Profanity Filter eliminates profanity and other offensive content from the web. | | | | | |
| NA | 09-02-2017 | 4.3 | An incorrect implementation of "XEP-0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This CVE is for profanity (0.4.7 - 0.5.0).<br>**REFERENCE: CVE-2017-5592** | NA | A-PRO-PROFA-280217/331 |
| **Psi-plus** | | | | | |
| ***Psi+***<br>Psi+ is a development branch of Psi IM Jabber client (Psi is a cross-platform powerful Jabber client (Qt, C++) designed for the Jabber power users). | | | | | |
| NA | 09-02-2017 | 4.3 | An incorrect implementation of "XEP-0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social | NA | A-PSI-PSI+-280217/332 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | engineering attacks. This CVE is for Psi+ (0.16.563.580 - 0.16.571.627).<br>**REFERENCE: CVE-2017-5593** | | |
| **Python** | | | | | |
| ***Openpyxl***<br>Openpyxl is a Python library for reading and writing Excel 2010 xlsx/xlsm/xltx/xltm files. | | | | | |
| NA | 15-02-2017 | 5.8 | Openpyxl 2.4.1 resolves external entities by default, which allows remote attackers to conduct XXE attacks via a crafted .xlsx document.<br>**REFERENCE: CVE-2017-5992** | https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=854442 | A-PYT-OPENP-280217/333 |
| **Saltstack** | | | | | |
| ***Salt***<br>Salt is a new approach to infrastructure management built on a dynamic communication bus. | | | | | |
| NA | 07-02-2017 | 7.5 | Salt before 2015.8.11 allows deleted minions to read or write to minions with the same id, related to caching.<br>**REFERENCE: CVE-2016-9639** | https://docs.saltstack.com/en/2015.8/ref/configuration/master.html#rotate-aes-key | A-SAL-SALT-280217/334 |
| **Sanadata** | | | | | |
| ***Sanacms***<br>Sana Software develops product software for eCommerce, eLearning and Web Content Management. | | | | | |
| Cross Site Scripting | 04-02-2017 | 4.3 | Cross-site scripting (XSS) vulnerability in index.asp in SANADATA SanaCMS 7.3 allows remote attackers to inject arbitrary web script or HTML via the search parameter.<br>**REFERENCE: CVE-2017-5882** | NA | A-SAN-SANAC-280217/335 |
| **SAP** | | | | | |
| ***Sap Kernel***<br>The SAP kernel is the core component of any SAP system. It consists of the executable files that run on the server to handle connections to the system and execute the SAP programs. | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Denial of Service | 15-02-2017 | 5 | The SAP Message Server HTTP daemon in SAP KERNEL 7.21-7.49 allows remote attackers to cause a denial of service (memory consumption and process crash) via multiple msgserver/group?group= requests with a crafted size of the group parameter, aka SAP Security Note 2358972.<br>**REFERENCE: CVE-2017-5997** | https://erpscan.com/advisories/erpscan-16-038-sap-message-server-http-remote-dos/ | A-SAP-SAPK-280217/336 |
| **Schneider-electric** | | | | | |
| ***Powerlogic Pm8ecc Firmware***<br>The PM8ECC is a communications add-on module for the Series 800 Power Meter that provides connectivity between Ethernet (Modbus TCP/IP) and serial line devices, allowing Modbus TCP/IP clients to access information from the host Power Meter and the serial slave devices. | | | | | |
| NA | 13-02-2017 | 7.5 | An issue was discovered in Schneider Electric PowerLogic PM8ECC device 2.651 and older. Undocumented hard-coded credentials allow access to the device.<br>**REFERENCE: CVE-2016-5818** | NA | A-SCH-POWER-280217/337 |
| **Simplemachines** | | | | | |
| ***Simple Machines Forum***<br>Simple Machines offers free open source software such as SMF, the powerful and easy to use community forum written in PHP. | | | | | |
| Execute Code | 09-02-2017 | 6.8 | LogInOut.php in Simple Machines Forum (SMF) 2.1 allows remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via vectors related to variables derived from user input in a foreach loop.<br>**REFERENCE: CVE-2016-5727** | https://github.com/SimpleMachines/SMF2.1/issues/3522 | A-SIM-SIMPL-280217/338 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| Execute Code | 09-02-2017 | 7.5 | Packages.php in Simple Machines Forum (SMF) 2.1 allows remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via the themechanges array parameter. **REFERENCE: CVE-2016-5726** | NA | A-SIM-SIMPL-280217/339 |
| **Simplesamlphp** |  |  |  |  |  |
| ***Simplesamlphp***<br>SimpleSAMLphp is an award-winning application written in native PHP that deals with authentication. |  |  |  |  |  |
| Gain Information | 07-02-2017 | 5 | The sanitycheck module in SimpleSAMLphp before 1.14.1 allows remote attackers to learn the PHP version on the system via unspecified vectors. **REFERENCE: CVE-2016-3124** | https://simplesamlphp.org/security/201603-01 | A-SIM-SIMPL-280217/340 |
| **Sleekxmpp Project; Slixmpp Project** |  |  |  |  |  |
| ***Sleekxmpp/Slixmpp***<br>A common use case for SleekXMPP is to send one-off messages from time to time/ Slixmpp is an MIT licensed XMPP library for Python 3.4+. |  |  |  |  |  |
| NA | 09-02-2017 | 4.3 | An incorrect implementation of "XEP-0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This CVE is for SleekXMPP up to 1.3.1 and Slixmpp all versions up to 1.2.3, as bundled in poezio (0.8 - 0.10) and other products. **REFERENCE: CVE-2017-5591** | NA | A-SLE-SLEEK-280217/341 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| **Sogo** | | | | | |
| ***Sogo***<br>Sogo is a fully supported and trusted groupware server with a focus on scalability and open standards. | | | | | |
| Denial of Service | 03-02-2017 | 6.8 | Memory leak in SOGo 2.3.7 allows remote attackers to cause a denial of service (memory consumption) via a large number of attempts to upload a large attachment, related to temporary files.<br>**REFERENCE: CVE-2016-6188** | https://github.com/inverse-inc/sogo/commit/32bb1456e23a32c7f45079c3985bf732dd0d276d | A-SOG-SOGO-280217/342 |
| **Squidguard** | | | | | |
| ***Squidguard***<br>SquidGuard is URL redirector software which can be used for content control of websites. | | | | | |
| Cross Site Scripting | 09-02-2017 | 4.3 | Cross-site scripting (XSS) vulnerability in squidGuard.cgi in squidGuard before 1.5 allows remote attackers to inject arbitrary web script or HTML via a blocked site link.<br>**REFERENCE: CVE-2015-8936** | http://www.squidguard.org/Downloads/Patches/1.4/Readme.Patch-20150201 | A-SQU-SQUID-280217/343 |
| **Videoinsight** | | | | | |
| ***Web Client***<br>The WebClient class provides common methods for sending data to or receiving data from any local, intranet, or Internet resource identified by a URI. | | | | | |
| Execute Code; SQL Injection | 13-02-2017 | 7.5 | An issue was discovered in VideoInsight Web Client Version 6.3.5.11 and previous versions. SQL Injection vulnerability has been identified, which may allow remote code execution.<br>**REFERENCE: CVE-2017-5151** | NA | A-VID-WEBC-280217/344 |
| **VIM** | | | | | |
| ***VIM***<br>Vim is an advanced text editor that seeks to provide the power of the de-facto Unix editor 'Vi', with a more complete feature set. | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Overflow | 10-02-2017 | 7.5 | vim before patch 8.0.0322 does not properly validate values for tree length when handling a spell file, which may result in an integer overflow at a memory allocation site and a resultant buffer overflow.<br>**REFERENCE: CVE-2017-5953** | https://github.com/vim/vim/commit/399c297aa93afe2c0a39e2a1b3f972aebba44c9d | A-VIM-VIM-280217/345 |
| **Visonic** | | | | | |
| ***Powerlink2 Firmware***<br>Visonic's PowerLink2 is the most comprehensive Internet-based solution for advanced home security and control. | | | | | |
| Cross Site Scripting | 13-02-2017 | 4.3 | An issue was discovered in Visonic PowerLink2, all versions prior to October 2016 firmware release. User controlled input is not neutralized prior to being placed in web page output (CROSS-SITE SCRIPTING).<br>**REFERENCE: CVE-2016-5811** | NA | A-VIS-POWER-280217/346 |
| **Webkit** | | | | | |
| ***Webkit***<br>WebKit is a layout engine software component for rendering web pages in web browsers. | | | | | |
| Denial of Service | 03-02-2017 | 4.3 | JavaScriptCore in WebKit allows attackers to cause a denial of service (out-of-bounds heap read) via a crafted Javascript file.<br>**REFERENCE: CVE-2016-9642** | NA | A-WEB-WEBKI-280217/347 |
| **Wordpress** | | | | | |
| ***Mail Plugin***<br>WP Mail plugin is simply a wp network mail or message system. Users can send mail or messages to other users over one wp network. | | | | | |
| Cross Site Scripting | 10-02-2017 | 4.3 | An issue was discovered in the WP Mail plugin before 1.2 for WordPress. The replyto parameter when composing a mail allows | https://cjc.im/advisories/0006/ | A-WOR-MAIL -280217/348 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | for a reflected XSS. This would allow you to execute JavaScript in the context of the user receiving the mail. **REFERENCE: CVE-2017-5942** | | |
| **Xabber** | | | | | |
| ***Xabber***<br>Xabber is the most popular open-source XMPP client for Android. | | | | | |
| NA | 09-02-2017 | 4.3 | An incorrect implementation of "XEP-0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This CVE is for Xabber (only if manually enabled: 1.0.30, 1.0.30 VIP, beta 1.0.3 - 1.0.74; Android). **REFERENCE: CVE-2017-5606** | NA | A-XAB-XABBE-280217/349 |
| **Yaxim** | | | | | |
| ***Bruno;Yaxim***<br>Bruno is a Jabber/XMPP Instant Messaging (IM) app and the themed version of the open source yaxim app; Yaxim is a Jabber/XMPP client with open source (GPLv2). | | | | | |
| NA | 09-02-2017 | 4.3 | An incorrect implementation of "XEP-0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This CVE is for yaxim and Bruno (0.8.6 - 0.8.8; Android). | NA | A-YAX-BRUNO-280217/350 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | **REFERENCE: CVE-2017-5589** | | |
| **Zoneminder** | | | | | |
| ***Zoneminder***<br>ZoneMinder is a free, open source Closed-circuit television software application developed for Linux. | | | | | |
| Gain Information File Inclusion | 06-02-2017 | 2.1 | A file disclosure and inclusion vulnerability exists in web/views/file.php in ZoneMinder 1.x through v1.30.0 because of unfiltered user-input being passed to readfile(), which allows an authenticated attacker to read local system files (e.g., /etc/passwd) in the context of the web server user (www-data). The attack vector is a .. (dot dot) in the path parameter within a zm/index.php?view=file&path= request.<br>**REFERENCE: CVE-2017-5595** | NA | A-ZON-ZONEM-280217/351 |
| Cross Site Scripting | 06-02-2017 | 4.3 | Multiple reflected XSS vulnerabilities exist within form and link input parameters of ZoneMinder v1.30 and v1.29, an open-source CCTV server web application, which allows a remote attacker to execute malicious scripts within an authenticated client's browser. The URL is /zm/index.php and sample parameters could include action=login&view=postlogin[XSS] view=console[XSS] view=groups[XSS] view=events&filter[terms] | NA | A-ZON-ZONEM-280217/352 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | [1][cnj]=and[XSS] view=events&filter%5Bterms%5D%5B1%5D%5Bcnj%5D=and[XSS] view=events&filter%5Bterms%5D%5B1%5D%5Bcnj%5D=[XSS]and view=events&limit=1%22%3E%3C/a%3E[XSS] (among others). **REFERENCE: CVE-2017-5367** |  |  |
| Cross Site Request Forgery | 06-02-2017 | 6.8 | ZoneMinder v1.30 and v1.29, an open-source CCTV server web application, is vulnerable to CSRF (Cross Site Request Forgery) which allows a remote attack to make changes to the web application as the current logged in victim. If the victim visits a malicious web page, the attacker can silently and automatically create a new admin user within the web application for remote persistence and further attacks. The URL is /zm/index.php and sample parameters could include action=user uid=0 newUser[Username]=attacker1 newUser[Password]=Password1234 conf_password=Password1234 newUser[System]=Edit (among others). **REFERENCE: CVE-2017-5368** | NA | A-ZON-ZONEM-280217/353 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| **Application; Operating System (A/OS)** | | | | | |
| **Canonical; Debian/ Exim** | | | | | |
| ***Ubuntu Linux/Debian Linux/Exim***<br>Ubuntu is a computer operating system based on the Debian Linux distribution and distributed as free and open source software, using its own desktop environment/ Debian is an operating system and a distribution of Free Software/ Exim is a mail transfer agent (MTA) used on Unix-like operating systems. | | | | | |
| NA | 01-02-2017 | 2.6 | Exim before 4.87.1 might allow remote attackers to obtain the private DKIM signing key via vectors related to log files and bounce messages.<br>**REFERENCE: CVE-2016-9963** | https://bugs.exim.org/show_bug.cgi?id=1996 | A-OS-CAN-UBUNT-280217/354 |
| **Debian; Fedoraproject/Jasper Project** | | | | | |
| ***Debian Linux/Fedora/Jasper***<br>Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License and packaged by a group of individuals participating in the Debian Project/ Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/ Jasper is an open source platform for developing always-on, voice-controlled applications. | | | | | |
| Denial of Service | 15-02-2017 | 4.3 | The jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.4 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted YRsiz value in a BMP image to the imginfo command.<br>**REFERENCE: CVE-2016-8692** | https://bugzilla.redhat.com/show_bug.cgi?id=1385502 | A-OS-DEB-DEBIA-280217/355 |
| Denial of Service | 15-02-2017 | 4.3 | The jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.4 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted XRsiz value in a | https://bugzilla.redhat.com/show_bug.cgi?id=1385502 | A-OS-DEB-DEBIA-280217/356 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | BMP image to the imginfo command.<br>**REFERENCE: CVE-2016-8691** | | |
| **Debian;Novell;Opensuse Project;Suse/Graphicsmagick;Suse** | | | | | |
| ***Debian Linux / Leap / Opensuse / Linux Enterprise Software Development Kit / Graphicsmagick / Linux Enterprise Debuginfo; Studio Onsite***<br>Debian is an operating system and a distribution of Free Software/ LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system/ openSUSE, formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies/ SUSE Linux Enterprise Software Development Kit 11 is a comprehensive development tool kit that is designed to support developers, as well as independent hardware vendors (IHVs) and independent software vendors (ISVs), in creating applications on or porting them to SUSE Linux Enterprise 11 products/ GraphicsMagick is the swiss army knife of image processing - comprised of 267K physical lines (according to David A. Wheeler's SLOCCount) of source code in the base package (or 1,225K including 3rd party libraries) it provides a robust and efficient collection of tools and libraries which support reading, writing, and manipulating an image in over 88 major formats including important formats like DPX, GIF, JPEG, JPEG-2000, PNG, PDF, PNM, and TIFF/ NA ; SUSE Studio Onsite is a Web application for building and testing appliances in a Web browser. | | | | | |
| Denial of Service | 03-02-2017 | 4.3 | GraphicsMagick 1.3.23 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted SVG file, related to the (1) DrawImage function in magick/render.c, (2) SVGStartElement function in coders/svg.c, and (3) TraceArcPath function in magick/render.c.<br>**REFERENCE: CVE-2016-2318** | https://bugzilla.redhat.com/show_bug.cgi?id=1306148 | A-OS-DEB-DEBIA-280217/357 |
| Denial of Service; Overflow | 03-02-2017 | 4.3 | Multiple buffer overflows in GraphicsMagick 1.3.23 allow remote attackers to cause a denial of service (crash) via a crafted SVG file, related to the (1) TracePoint function in magick/render.c, (2) GetToken function in magick/utility.c, and (3) GetTransformTokens function in coders/svg.c. | https://bugzilla.redhat.com/show_bug.cgi?id=1306148 | A-OS-DEB-DEBIA-280217/358 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | **REFERENCE: CVE-2016-2317** |  |  |
| **Debian;Novell;Opensuse Project/Graphicsmagick** |  |  |  |  |  |
| ***Debian Linux/Leap/Opensuse/Graphicsmagick***<br>Debian is an operating system and a distribution of Free Software/ LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system/ openSUSE, formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies/ GraphicsMagick is the swiss army knife of image processing - comprised of 267K physical lines (according to David A. Wheeler's SLOCCount) of source code in the base package (or 1,225K including 3rd party libraries) it provides a robust and efficient collection of tools and libraries which support reading, writing, and manipulating an image in over 88 major formats including important formats like DPX, GIF, JPEG, JPEG-2000, PNG, PDF, PNM, and TIFF. |  |  |  |  |  |
| Denial of Service; Overflow | 06-02-2017 | 5 | Integer underflow in the parse8BIM function in coders/meta.c in GraphicsMagick 1.3.25 and earlier allows remote attackers to cause a denial of service (application crash) via a crafted 8BIM chunk, which triggers a heap-based buffer overflow.<br>**REFERENCE: CVE-2016-7800** | https://sourceforge.net/p/graphicsmagick/code/ci/5c7b6d6094a25e99c57f8b18343914ebfd8213ef/ | A-OS-DEB-DEBIA-280217/359 |
| **Debian; Novell/ Littlecms** |  |  |  |  |  |
| ***Debian Linux/Leap/Little Cms Color Engine***<br>Debian is an operating system and a distribution of Free Software/ Exim is a mail transfer agent (MTA) used on Unix-like operating systems/ LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system / Little Cms Color Engine is a free, open source, CMM engine and provides fast transforms between ICC profiles |  |  |  |  |  |
| Denial of Service; Gain Information | 03-02-2017 | 5.8 | The Type_MLU_Read function in cmstypes.c in Little CMS (aka lcms2) allows remote attackers to obtain sensitive information or cause a denial of service via an image with a crafted ICC profile, which triggers an out-of-bounds heap read.<br>**REFERENCE: CVE-2016-10165** | https://github.com/mm2/Little-CMS/commit/5ca71a7bc18b6897ab21d815d15e218e204581e2 | A-OS-DEB-DEBIA-280217/360 |
| **Debian; Opensuse Project / Graphicsmagick** |  |  |  |  |  |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| ***Debian Linux / Opensuse / Graphicsmagick***<br>Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License and packaged by a group of individuals participating in the Debian Project / openSUSE, formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies / GraphicsMagick is the swiss army knife of image processing - comprised of 267K physical lines (according to David A. Wheeler's SLOCCount) of source code in the base package (or 1,225K including 3rd party libraries) it provides a robust and efficient collection of tools and libraries which support reading, writing, and manipulating an image in over 88 major formats including important formats like DPX, GIF, JPEG, JPEG-2000, PNG, PDF, PNM, and TIFF. | | | | | |
| Denial of Service | 15-02-2017 | 5 | The ReadSCTImage function in coders/sct.c in GraphicsMagick 1.3.25 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted SCT header.<br>**REFERENCE: CVE-2016-8682** | https://bugzilla.redhat.com/show_bug.cgi?id=1385583 | A-OS-DEB-DEBIA-280217/361 |
| Overflow | 15-02-2017 | 6.8 | The MagickMalloc function in magick/memory.c in GraphicsMagick 1.3.25 allows remote attackers to have unspecified impact via a crafted image, which triggers a memory allocation failure and a "file truncation error for corrupt file."<br>**REFERENCE: CVE-2016-8684** | https://bugzilla.redhat.com/show_bug.cgi?id=1385583 | A-OS-DEB-DEBIA-280217/362 |
| Overflow | 15-02-2017 | 6.8 | The ReadPCXImage function in coders/pcx.c in GraphicsMagick 1.3.25 allows remote attackers to have unspecified impact via a crafted image, which triggers a memory allocation failure and a "file truncation error for corrupt file."<br>**REFERENCE: CVE-2016-8683** | http://hg.code.sf.net/p/graphicsmagick/code/rev/b9edafd479b9 | A-OS-DEB-DEBIA-280217/363 |
| **Debian;Opensuse Project/Imagemagick** | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| ***Debian Linux/Opensuse/Imagemagick***<br>Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License and packaged by a group of individuals participating in the Debian Project / openSUSE, formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies / ImageMagick is a software suite to create, edit, compose, or convert bitmap images. | | | | | |
| Overflow | 15-02-2017 | 6.8 | The AcquireQuantumPixels function in MagickCore/quantum.c in ImageMagick before 7.0.3-1 allows remote attackers to have unspecified impact via a crafted image file, which triggers a memory allocation failure.<br>**REFERENCE: CVE-2016-8677** | https://github.com/ImageMagick/ImageMagick/issues/268 | A-OS-DEB-DEBIA-280217/364 |
| **Debian/Dicom** | | | | | |
| ***Debian Linux/Dcmtk***<br>Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License and packaged by a group of individuals participating in the Debian Project / DCMTK is a collection of libraries and applications implementing large parts the DICOM standard | | | | | |
| Denial of Service; Overflow | 15-02-2017 | 5 | Stack-based buffer overflow in the parsePresentationContext function in storescp in DICOM dcmtk-3.6.0 and earlier allows remote attackers to cause a denial of service (segmentation fault) via a long string sent to TCP port 4242.<br>**REFERENCE: CVE-2015-8979** | https://bugzilla.redhat.com/show_bug.cgi?id=1405919 | A-OS-DEB-DEBIA-280217/365 |
| **Debian / Graphicsmagick** | | | | | |
| ***Debian Linux / Graphicsmagick***<br>Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License and packaged by a group of individuals participating in the Debian Project / GraphicsMagick is the swiss army knife of image processing- comprised of 267K physical lines (according to David A. Wheeler's SLOCCount) of source code in the base package (or 1,225K including 3rd party libraries) it provides a robust and efficient collection of tools and libraries which support reading, writing, and manipulating an image in over 88 major formats including important formats like DPX, GIF, JPEG, JPEG-2000, PNG, PDF, PNM, and TIFF. | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Overflow | 15-02-2017 | 6.8 | The AcquireMagickMemory function in MagickCore/memory.c in GraphicsMagick before 7.0.3.3 allows remote attackers to have unspecified impact via a crafted image, which triggers a memory allocation failure.<br>**REFERENCE: CVE-2016-8862** | https://bugzilla.redhat.com/show_bug.cgi?id=1387135 | A-OS-DEB-DEBIA-280217/366 |
| **Debian/Libtiff** | | | | | |
| ***Debian Linux/Libtiff***<br>Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License and packaged by a group of individuals participating in the Debian Project / Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files. | | | | | |
| Denial of Service; Overflow | 06-02-2017 | 4.3 | Integer overflow in the writeBufferToSeparateStrips function in tiffcrop.c in LibTIFF before 4.0.7 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tif file.<br>**REFERENCE: CVE-2016-9532** | https://bugzilla.redhat.com/show_bug.cgi?id=1397726 | A-OS-DEB-DEBIA-280217/367 |
| **Fedoraproject;Novell;Opensuse Project;Suse/Libgit2 Project** | | | | | |
| ***Fedora/Leap/Leap;Opensuse/Linux Enterprise/Libgit2***<br>Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/ LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system; OpenSUSE, formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies/ SUSE Linux Enterprise Desktop delivers essential office functionality affordably, and was built to coexist with other operating systems/ libgit2 is a portable, pure C implementation of the Git core methods provided as a re-entrant linkable library with a solid API, allowing you to write native speed custom Git applications in any language which supports C bindings. | | | | | |
| Denial of Service | 03-02-2017 | 4.3 | The git_oid_nfmt function in commit.c in libgit2 before 0.24.3 allows remote attackers to cause a denial of service (NULL | https://bugzilla.redhat.com/show_bug.cgi?id=1383211 | A-OS-FED-FEDOR-280217/368 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | pointer dereference) via a cat-file command with a crafted object file.<br>**REFERENCE: CVE-2016-8569** | | |
| Denial of Service | 03-02-2017 | 4.3 | The git_commit_message function in oid.c in libgit2 before 0.24.3 allows remote attackers to cause a denial of service (out-of-bounds read) via a cat-file command with a crafted object file.<br>**REFERENCE: CVE-2016-8568** | https://bugzilla.redhat.com/show_bug.cgi?id=1383211 | A-OS-FED-FEDOR-280217/369 |
| **Fedoraproject;Opensuse Project/Jasper Project** | | | | | |
| ***Fedora/Opensuse/Jasper***<br>Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/ openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies/Jasper is an open source platform for developing always-on, voice-controlled applications. | | | | | |
| Denial of Service; Execute Code | 15-02-2017 | 6.8 | Double free vulnerability in the mem_close function in jas_stream.c in JasPer before 1.900.10 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted BMP image to the imginfo command.<br>**REFERENCE: CVE-2016-8693** | https://bugzilla.redhat.com/show_bug.cgi?id=1385507 | A-OS-FED-FEDOR-280217/370 |
| **Fedoraproject/Jasper Project** | | | | | |
| ***Fedora/Jasper***<br>Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat /Jasper is an open source platform for developing always-on, voice-controlled applications. | | | | | |
| Denial of Service | 15-02-2017 | 4.3 | The bmp_getdata function in libjasper/bmp/bmp_dec.c in JasPer before 1.900.5 allows remote attackers to cause a denial of service | https://bugzilla.redhat.com/show_bug.cgi?id=1385499 | A-OS-FED-FEDOR-280217/371 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | (NULL pointer dereference) via a crafted BMP image in an imginfo command.<br>**REFERENCE: CVE-2016-8690** | | |
| **Fedoraproject/Libwebp Project** | | | | | |
| ***Fedora/Libwebp***<br>Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/ The libwebp package contains a library and support programs to encode and decode images in WebP format. | | | | | |
| Overflow | 03-02-2017 | 7.5 | Multiple integer overflows in libwebp allows attackers to have unspecified impact via unknown vectors.<br>**REFERENCE: CVE-2016-9085** | https://bugzilla.redhat.com/show_bug.cgi?id=1389338 | A-OS-FED-FEDOR-280217/372 |
| **Fedoraproject/Openjpeg** | | | | | |
| ***Fedora/Openjpeg***<br>Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/OpenJPEG is an open-source library to encode and decode JPEG 2000 images. | | | | | |
| Denial of Service | 03-02-2017 | 4.3 | Divide-by-zero vulnerability in the opj_tcd_init_tile function in tcd.c in OpenJPEG before 2.1.1 allows remote attackers to cause a denial of service (application crash) via a crafted jp2 file. NOTE: this issue exists because of an incorrect fix for REFERENCE: CVE-2014-7947.<br>**REFERENCE: CVE-2016-4797** | https://bugzilla.redhat.com/show_bug.cgi?id=1335483 | A-OS-FED-FEDOR-280217/373 |
| Denial of Service; Overflow | 03-02-2017 | 4.3 | Heap-based buffer overflow in the color_cmyk_to_rgb in common/color.c in OpenJPEG before 2.1.1 allows remote attackers to cause a denial of service | https://bugzilla.redhat.com/show_bug.cgi?id=1335482 | A-OS-FED-FEDOR-280217/374 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | (crash) via a crafted .j2k file.<br>**REFERENCE: CVE-2016-4796** | | |
| **Fedoraproject/Suckless** | | | | | |
| ***Fedora/Slock***<br>Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/ Slock- Simple X display locker-This is the simplest X screen locker. | | | | | |
| Bypass | 15-02-2017 | 5 | Slock allows attackers to bypass the screen lock via vectors involving an invalid password hash, which triggers a NULL pointer dereference and crash.<br>**REFERENCE: CVE-2016-6866** | http://git.suckless.org/slock/commit/?id=d8bec0f6fdc8a246d78cb488a0068954b46fcb29 | A-OS-FED-FEDOR-280217/375 |
| **IBM/IBM** | | | | | |
| ***Security Access Manager 9.0 Firmware;Security Access Manager For Web 7.0 Firmware;Security Access Manager For Web 8.0 Firmware/Security Access Manager For Mobile***<br>IBM Security Access Manager enables businesses to more securely adopt web, mobile, and cloud technologies and simplifies user access management for employees and consumers. | | | | | |
| Gain Information | 01-02-2017 | 4.3 | IBM Security Access Manager for Web could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.<br>**REFERENCE: CVE-2016-3043** | http://www.ibm.com/support/docview.wss?uid=swg21995446 | A-OS-IBM-SECUR-280217/376 |
| Bypass | 07-02-2017 | 4.3 | IBM Security Access Manager for Web 7.0.0, 8.0.0, and 9.0.0 could allow a remote attacker to bypass security restrictions, caused by improper content validation. By persuading | http://www.ibm.com/support/docview.wss?uid=swg21996826 | A-OS-IBM-SECUR-280217/377 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | a victim to open specially-crafted content, an attacker could exploit this vulnerability to bypass validation and load a page with malicious content. **REFERENCE: CVE-2016-3020** | | |
| Gain Information | 08-02-2017 | 2.1 | The IBM Security Access Manager appliance includes configuration files that contain obfuscated plaintext-passwords which authenticated users can access. **REFERENCE: CVE-2015-5013** | http://www.ibm.com/support/docview.wss?uid=swg21993722 | A-OS-IBM-SECUR-280217/378 |
| SQL Injection | 01-02-2017 | 4 | IBM Security Access Manager for Web is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements which could allow the attacker to view information in the back-end database. **REFERENCE: CVE-2016-3046** | http://www.ibm.com/support/docview.wss?uid=swg21995527 | A-OS-IBM-SECUR-280217/379 |
| **Libarchive/Opensuse Project** | | | | | |
| ***Libarchive/Leap***<br>The libarchive library provides a single interface for reading/writing various compression formats/ LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system. | | | | | |
| Denial of Service | 15-02-2017 | 4.3 | The mtree bidder in libarchive 3.2.1 does not keep track of line sizes when extending the read-ahead, which allows remote attackers to cause a denial of service (crash) via a crafted file, which triggers an invalid read in the (1) detect_form or (2) | https://github.com/libarchive/libarchive/commit/eec077f52bfa2d3f7103b4b74d52572ba8a15aca | A-OS-LIB-LIBAR-280217/380 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | bid_entry function in libarchive/archive_read_support_format_mtree.c. **REFERENCE: CVE-2016-8688** | | |
| **Moxa/Moxa** | | | | | |
| ***Nport 5100 Series Firmware;Nport 5100a Series Firmware;Nport 5200 Series Firmware;Nport 5200a Series Firmware;Nport 5400 Series Firmware;Nport 5600 Series Firmware;Nport 5x50a1-m12 Series Firmware;Nport 6100 Series Firmware;Nport P5150a Series Firmware/Nport 5600-8-dtl Series Firmware***<br>The MOXA NPort 5000 and 6000 Series device allows a Serial GSM modem to be connected to a Swivel appliance through an ethernet network connection. Since 2002, Moxa has continued to grow at a rate of about 30% each year. A branch office has been opened in Europe, and Moxa's product offerings have expanded to include managed industrial Ethernet switches, embedded computers, and industrial wireless solutions. | | | | | |
| NA | 13-02-2017 | 7.8 | An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. The amount of resources requested by | NA | A-OS-MOX-NPORT-280217/381 |

| CV Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | a malicious actor is not restricted, leading to a denial-of-service caused by resource exhaustion. **REFERENCE: CVE-2016-9367** | | |
| **Artifex / Fedoraproject** | | | | | |
| ***Mujs / Fedora*** MuJS is a lightweight Javascript interpreter designed for embedding in other software to extend them with scripting capabilities/ Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project. | | | | | |
| Denial of Service; Overflow | 03-02-2017 | 5 | Integer overflow in the js_regcomp function in regexp.c in Artifex Software, Inc. MuJS before commit b6de34ac6d8bb7dd5461c57940acfbd3ee7fd93e allows attackers to cause a denial of service (application crash) via a crafted regular expression. **REFERENCE: CVE-2016-9108** | https://bugzilla.redhat.com/show_bug.cgi?id=1390266 | A-OS-ART-MUJS/-280217/382 |
| **Dlitz/Fedoraproject** | | | | | |
| ***Pycrypto/Fedora*** PyCrypto is alibrary, which provides secure hash functions and various encryption algorithms/ Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project. | | | | | |
| Execute Code; Overflow | 15-02-2017 | 7.5 | Heap-based buffer overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted iv parameter to cryptmsg.py. **REFERENCE: CVE-2013-7459** | https://github.com/dlitz/pycrypto/issues/176 | A-OS-DLI-PYCRY-280217/383 |
| **Graphicsmagick/Novell;Opensuse Project** | | | | | |
| ***Graphicsmagick/Leap/Opensuse*** GraphicsMagick is the swiss army knife of image processing - comprised of 267K physical lines | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| (according to David A. Wheeler's SLOCCount) of source code in the base package (or 1,225K including 3rd party libraries) it provides a robust and efficient collection of tools and libraries which support reading, writing, and manipulating an image in over 88 major formats including important formats like DPX, GIF, JPEG, JPEG-2000, PNG, PDF, PNM, and TIFF/ LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system / openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies/ | | | | | |
| Denial of Service | 03-02-2017 | 4.3 | magick/render.c in GraphicsMagick before 1.3.24 allows remote attackers to cause a denial of service (arithmetic exception and application crash) via a crafted svg file.<br>**REFERENCE: CVE-2016-5241** | https://bugzilla.redhat.com/show_bug.cgi?id=1333410 | A-OS-GRA-GRAPH-280217/384 |
| Denial of Service | 06-02-2017 | 5 | The TIFFGetField function in coders/tiff.c in GraphicsMagick 1.3.24 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a file containing an "unterminated" string.<br>**REFERENCE: CVE-2016-7449** | https://bugzilla.redhat.com/show_bug.cgi?id=1374233 | A-OS-GRA-GRAPH-280217/385 |
| Overflow | 06-02-2017 | 7.5 | Heap-based buffer overflow in the EscapeParenthesis function in GraphicsMagick before 1.3.25 allows remote attackers to have unspecified impact via unknown vectors.<br>**REFERENCE: CVE-2016-7447** | https://bugzilla.redhat.com/show_bug.cgi?id=1374233 | A-OS-GRA-GRAPH-280217/386 |
| Overflow | 06-02-2017 | 7.5 | Buffer overflow in the MVG and SVG rendering code in GraphicsMagick 1.3.24 allows remote attackers to have unspecified impact via unknown vectors. Note: | https://bugzilla.redhat.com/show_bug.cgi?id=1374233 | A-OS-GRA-GRAPH-280217/387 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | This vulnerability exists due to an incomplete patch for CVE-2016-2317. **REFERENCE: CVE-2016-7446** |  |  |
| Denial of Service | 06-02-2017 | 7.8 | The Utah RLE reader in GraphicsMagick before 1.3.25 allows remote attackers to cause a denial of service (CPU consumption or large memory allocations) via vectors involving the header information and the file size. **REFERENCE: CVE-2016-7448** | https://bugzilla.redhat.com/show_bug.cgi?id=1374233 | A-OS-GRA-GRAPH-280217/388 |
| **Libarchive/Opensuse Project** |  |  |  |  |  |
| ***Libarchive/Leap***<br>The libarchive library provides a single interface for reading/writing various compression formats/ LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system. |  |  |  |  |  |
| Denial of Service | 15-02-2017 | 5 | The read_Header function in archive_read_support_format_7zip.c in libarchive 3.2.1 allows remote attackers to cause a denial of service (out-of-bounds read) via multiple EmptyStream attributes in a header in a 7zip archive. **REFERENCE: CVE-2016-8689** | https://bugzilla.redhat.com/show_bug.cgi?id=1377925 | A-OS-LIB-LIBAR-280217/389 |
| Denial of Service; Overflow | 15-02-2017 | 5 | Stack-based buffer overflow in the safe_fprintf function in tar/util.c in libarchive 3.2.1 allows remote attackers to cause a denial of service via a crafted non-printable multibyte character in a filename. **REFERENCE: CVE-2016-8687** | https://bugzilla.redhat.com/show_bug.cgi?id=1377926 | A-OS-LIB-LIBAR-280217/390 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| **Application; Hardware (A/H)** | | | | | |
| **F5/F5** | | | | | |
| ***Big-ip Access Policy Manager; Big-ip Advanced Firewall Manager; Big-ip Analytics; Big-ip Application Acceleration Manager; Big-ip Application Security Manager; Big-ip Global Traffic Manager; Big-ip Link Controller; Big-ip Local Traffic Manager; Big-ip Policy Enforcement Manager/ Big-ip Protocol Security Manager***<br>BIG-IP System - A blend of software and hardware gives you the ability to control the traffic that passes through your network. | | | | | |
| Gain Information | 09-02-2017 | 5 | A BIG-IP virtual server configured with a Client SSL profile that has the non-default Session Tickets option enabled may leak up to 31 bytes of uninitialized memory. A remote attacker may exploit this vulnerability to obtain Secure Sockets Layer (SSL) session IDs from other sessions. It is possible that other data from uninitialized memory may be returned as well.<br>**REFERENCE: CVE-2016-9244** | https://support.f5.com/csp/article/K05121675 | A-H-F5/-BIG-I-280217/391 |
| **Hardware (H)** | | | | | |
| **Cisco** | | | | | |
| ***Industrial Ethernet 2000 Series Firmware***<br>Cisco Industrial Ethernet 2000 (IE 2000) Series Switches extend the proven Cisco Catalyst technologies prevalent in enterprise networks to industrial networks. | | | | | |
| Denial of Service; Gain Information | 03-02-2017 | 7.1 | A vulnerability in the implementation of Common Industrial Protocol (CIP) functionality in Cisco Industrial Ethernet 2000 Series Switches could allow an unauthenticated, remote attacker to cause a | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-psc1 | H-CIS-INDUS-280217/392 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | denial of service (DoS) condition due to a system memory leak. More Information: CSCvc54788. Known Affected Releases: 15.2(5.4.32i)E2. Known Fixed Releases: 15.2(5.4.62i)E2. **REFERENCE: CVE-2017-3812** | | |
| **Fortinet** | | | | | |
| ***Fortiwlc***<br>The FortiWLC controller series optimizes traffic across infrastructure wireless access points and client devices to support high density, high performance and predictability while addressing mission-critical enterprise demands for wireless connectivity. | | | | | |
| NA | 01-02-2017 | 9.4 | The presence of a hardcoded account named 'core' in Fortinet FortiWLC allows attackers to gain unauthorized read/write access via a remote shell. **REFERENCE: CVE-2016-8491** | https://fortiguard.com/advisory/FG-IR-16-065 | H-FOR-FORTI-280217/393 |
| **Hardware; Operating System (H/OS)** | | | | | |
| **Moxa/Moxa** | | | | | |
| ***Nport 5100 Series Firmware; Nport 5100a Series Firmware; Nport 5200 Series Firmware; Nport 5200a Series Firmware; Nport 5400 Series Firmware; Nport 5600 Series Firmware; Nport 5x50a1-m12 Series Firmware; Nport 6100 Series Firmware;Nport P5150a Series Firmware/ Nport 5600-8-dtl Series Firmware***<br>The MOXA NPort 5000 and 6000 Series devices allow a Serial GSM modem to be connected to a Swivel appliance through an ethernet network connection. Since 2002, Moxa has continued to grow at a rate of about 30% each year. A branch office has been opened in Europe, and Moxa's product offerings have expanded to include managed industrial Ethernet switches, embedded computers, and industrial wireless solutions. | | | | | |
| NA | 13-02-2017 | 2.1 | An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series | NA | H-OS-MOX-NPORT-280217/394 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. A configuration file contains parameters that represent passwords in plaintext. **REFERENCE: CVE-2016-9348** | | |
| Cross Site Scripting | 13-02-2017 | 4.3 | An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to | NA | H-OS-MOX-NPORT-280217/395 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. User-controlled input is not neutralized before being output to web page (CROSS-SITE SCRIPTING). **REFERENCE: CVE-2016-9371** | | |
| Bypass | 13-02-2017 | 5 | An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. An attacker can freely use brute force to determine parameters | NA | H-OS-MOX-NPORT-280217/396 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | needed to bypass authentication. **REFERENCE: CVE-2016-9366** | | |
| Cross Site Request Forgery | 13-02-2017 | 6.8 | An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. Requests are not verified to be intentionally submitted by the proper user (CROSS-SITE REQUEST FORGERY). **REFERENCE: CVE-2016-9365** | NA | H-OS-MOX-NPORT-280217/397 |
| Execute Code; Overflow | 13-02-2017 | 7.5 | An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series | NA | H-OS-MOX-NPORT-280217/398 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. Buffer overflow vulnerability may allow an unauthenticated attacker to remotely execute arbitrary code. **REFERENCE: CVE-2016-9363** |  |  |
| NA | 13-02-2017 | 7.5 | An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to | NA | H-OS-MOX-NPORT-280217/399 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. Administration passwords can be retried without authenticating. **REFERENCE: CVE-2016-9361** | | |
| Execute Code | 13-02-2017 | 10 | An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series | NA | H-OS-MOX-NPORT-280217/400 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. Firmware can be updated over the network without authentication, which may allow remote code execution.<br>**REFERENCE: CVE-2016-9369** |  |  |
| **Operating System (OS)** |  |  |  |  |  |
| **Adcon Telemetry** |  |  |  |  |  |
| ***A850 Telemetry Gateway Base Station Firmware***<br>The A850 Telemetry Gateway is the core of every Adcon monitoring network, be it a pure GSM / GPRS network, a UHF radio network or a combination of both – it is the A850 that knows exactly when and how to retrieve data from each RTU. |  |  |  |  |  |
| Cross Site Scripting | 13-02-2017 | 4.3 | An issue was discovered in Adcon Telemetry A850 Telemetry Gateway Base Station. The Web Interface does not neutralize or incorrectly neutralizes user-controllable input before it is placed in the output; this could allow for cross-site scripting.<br>**REFERENCE: CVE-2016-2274** | NA | O-ADC-A850 - 280217/401 |
| **Binom3** |  |  |  |  |  |
| ***Universal Multifunctional Electric Power Quality Meter Firmware***<br>NA |  |  |  |  |  |
| Execute Code; Cross Site Scripting | 13-02-2017 | 4.3 | An issue was discovered in BINOM3 Universal Multifunctional Electric Power Quality Meter. Input sent from a malicious client is not properly verified by the server. An attacker can execute arbitrary script code in another user's browser session (CROSS-SITE SCRIPTING).<br>**REFERENCE: CVE-2017-** | NA | O-BIN-UNIVE-280217/402 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | **5164** | | |
| Gain Privileges; Gain Information | 13-02-2017 | 5 | An issue was discovered in BINOM3 Universal Multifunctional Electric Power Quality Meter. An INFORMATION EXPOSURE flaw can be used to gain privileged access to the device. **REFERENCE: CVE-2017-5166** | NA | O-BIN-UNIVE-280217/403 |
| Cross Site Request Forgery | 13-02-2017 | 6.8 | An issue was discovered in BINOM3 Universal Multifunctional Electric Power Quality Meter. There is no CSRF Token generated per page and/or per (sensitive) function. Successful exploitation of this vulnerability can allow silent execution of unauthorized actions on the device such as configuration parameter changes, and saving modified configuration. **REFERENCE: CVE-2017-5165** | NA | O-BIN-UNIVE-280217/404 |
| NA | 13-02-2017 | 7.5 | An issue was discovered in BINOM3 Universal Multifunctional Electric Power Quality Meter. Users do not have any option to change their own passwords. **REFERENCE: CVE-2017-5167** | NA | O-BIN-UNIVE-280217/405 |
| NA | 13-02-2017 | 10 | An issue was discovered in BINOM3 Universal Multifunctional Electric Power Quality Meter. Lack of authentication for remote service gives access to application set | NA | O-BIN-UNIVE-280217/406 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | up and configuration.<br>**REFERENCE: CVE-2017-5162** |  |  |
| **Carlosgavazzi** |  |  |  |  |  |
| ***Vmu-c Em Firmware;Vmu-c Pv Firmware***<br>VMUC EM- the WebServer Solution for any energy management applications; VMUC PV- for the PhotoVoltaic Monitoring systems |  |  |  |  |  |
| Gain Information | 13-02-2017 | 5 | An issue was discovered in Carlo Gavazzi VMU-C EM prior to firmware Version A11_U05, and VMU-C PV prior to firmware Version A17. Sensitive information is stored in clear-text.<br>**REFERENCE: CVE-2017-5146** | NA | O-CAR-VMU-C-280217/407 |
| Cross Site Request Forgery | 13-02-2017 | 7.5 | An issue was discovered in Carlo Gavazzi VMU-C EM prior to firmware Version A11_U05, and VMU-C PV prior to firmware Version A17. Successful exploitation of this CROSS-SITE REQUEST FORGERY (CSRF) vulnerability can allow execution of unauthorized actions on the device such as configuration parameter changes, and saving modified configuration.<br>**REFERENCE: CVE-2017-5145** | NA | O-CAR-VMU-C-280217/408 |
| NA | 13-02-2017 | 7.5 | An issue was discovered in Carlo Gavazzi VMU-C EM prior to firmware Version A11_U05, and VMU-C PV prior to firmware Version A17. The access control flaw allows access to most application functions without authentication.<br>**REFERENCE: CVE-2017-5144** | NA | O-CAR-VMU-C-280217/409 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| **Cisco** | | | | | |
| ***Ios Xe***<br>Cisco IOS XE software provides a modular structure that significantly enhances software quality and performance by separating the data plane and control plan. | | | | | |
| Denial of Service; Overflow | 03-02-2017 | 5.4 | A vulnerability in the handling of list headers in Cisco cBR Series Converged Broadband Routers could allow an unauthenticated, remote attacker to cause the device to reload, resulting in a denial of service (DoS) condition. Cisco cBR-8 Converged Broadband Routers running vulnerable versions of Cisco IOS XE are affected. More Information: CSCux40637. Known Affected Releases: 15.5(3)S 15.6(1)S. Known Fixed Releases: 15.5(3)S2 15.6(1)S1 15.6(2)S 15.6(2)SP 16.4(1). **REFERENCE: CVE-2017-3824** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-cbr | O-CIS-IOS X-280217/410 |
| **Fidelex** | | | | | |
| ***Fx-2030a Firmware;Fx-2030a-basic Firmware***<br>NA | | | | | |
| Directory Traversal | 13-02-2017 | 5 | An issue was discovered in Fidelix FX-20 series controllers, versions prior to 11.50.19. Arbitrary file reading via path traversal allows an attacker to access arbitrary files and directories on the server. **REFERENCE: CVE-2016-9364** | NA | O-FID-FX-20-280217/411 |
| **Freebsd** | | | | | |
| ***Freebsd***<br>FreeBSD is an operating system for a variety of platforms which focuses on features, speed, and stability. | | | | | |
| Gain | 07-02-2017 | 2.1 | bsnmpd, as used in | https://pierreki | O-FRE- |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Information | | | FreeBSD 9.3, 10.1, and 10.2, uses world-readable permissions on the snmpd.config file, which allows local users to obtain the secret key for USM authentication by reading the file. **REFERENCE: CVE-2015-5677** | m.github.io/blog/2016-01-15-Reference: CVE-2015-5677-freebsd-bsnmpd.html | FREEB-280217/412 |
| Bypass | 15-02-2017 | 5 | The telnetd service in FreeBSD 9.3, 10.1, 10.2, 10.3, and 11.0 allows remote attackers to inject arguments to login and bypass authentication via vectors involving a "sequence of memory allocation failures." **REFERENCE: CVE-2016-1888** | NA | O-FRE-FREEB-280217/413 |
| Overflow; Gain Privileges | 15-02-2017 | 7.2 | Integer overflow in the bhyve hypervisor in FreeBSD 10.1, 10.2, 10.3, and 11.0 when configured with a large amount of guest memory, allows local users to gain privilege via a crafted device descriptor. **REFERENCE: CVE-2016-1889** | NA | O-FRE-FREEB-280217/414 |
| Gain Privileges | 15-02-2017 | 7.2 | The issetugid system call in the Linux compatibility layer in FreeBSD 9.3, 10.1, and 10.2 allows local users to gain privilege via unspecified vectors. **REFERENCE: CVE-2016-1883** | NA | O-FRE-FREEB-280217/415 |
| Denial of Service; Gain Privileges | 15-02-2017 | 7.2 | The kernel in FreeBSD 9.3, 10.1, and 10.2 allows local users to cause a denial of service (crash) or potentially gain privilege | NA | O-FRE-FREEB-280217/416 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | via a crafted Linux compatibility layer setgroups system call. **REFERENCE: CVE-2016-1881** | | |
| Gain Privileges | 15-02-2017 | 7.2 | The Linux compatibility layer in the kernel in FreeBSD 9.3, 10.1, and 10.2 allows local users to read portions of kernel memory and potentially gain privilege via unspecified vectors, related to "handling of Linux futex robust lists." **REFERENCE: CVE-2016-1880** | NA | O-FRE-FREEB-280217/417 |
| **Google** | | | | | |
| ***Android***<br>Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets. | | | | | |
| NA | 08-02-2017 | 2.9 | An elevation of privilege vulnerability in Bluetooth could enable a proximate attacker to manage access to documents on the device. This issue is rated as Moderate because it first requires exploitation of a separate vulnerability in the Bluetooth stack. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32612586. **REFERENCE: CVE-2017-0423** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/418 |
| Gain Information | 08-02-2017 | 4.3 | An information disclosure vulnerability in the Filesystem could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/419 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | access sensitive data without permission. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-32799236. **REFERENCE: CVE-2017-0426** | | |
| Gain Information | 08-02-2017 | 4.3 | An information disclosure vulnerability in Audioserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access sensitive data without permission. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32720785. **REFERENCE: CVE-2017-0425** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/420 |
| Bypass; Gain Information | 08-02-2017 | 4.3 | An information disclosure vulnerability in AOSP Messaging could enable a remote attacker using a special crafted file to access data outside of its permission levels. This issue is rated as Moderate because it is a general bypass for a user level defense in depth or exploit mitigation technology in a privileged process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32322450. **REFERENCE: CVE-2017-0424** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/421 |
| Bypass; Gain Information | 08-02-2017 | 4.3 | An information disclosure vulnerability in the | https://source.android.com/se | O-GOO-ANDRO- |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | Framework APIs could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32555637. **REFERENCE: CVE-2017-0421** | curity/bulletin/01-02-2017.html | 280217/422 |
| Bypass; Gain Information | 08-02-2017 | 4.3 | An information disclosure vulnerability in AOSP Mail could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32615212. **REFERENCE: CVE-2017-0420** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/423 |
| Bypass; Gain Information | 08-02-2017 | 4.3 | An information disclosure vulnerability in AOSP Messaging could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/424 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32807795. **REFERENCE: CVE-2017-0414** | | |
| Bypass; Gain Information | 08-02-2017 | 4.3 | An information disclosure vulnerability in AOSP Messaging could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32161610. **REFERENCE: CVE-2017-0413** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/425 |
| Execute Code | 08-02-2017 | 6.8 | A remote code execution vulnerability in libstagefright could enable an attacker using a specially crafted file to execute arbitrary code in the context of an unprivileged process. This issue is rated as High due to the possibility of remote code execution in an application that uses this library. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-31999646. **REFERENCE: CVE-2017-0409** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/426 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| Execute Code | 08-02-2017 | 6.8 | A remote code execution vulnerability in libgdx could enable an attacker using a specially crafted file to execute arbitrary code in the context of an unprivileged process. This issue is rated as High due to the possibility of remote code execution in an application that uses this library. Product: Android. Versions: 7.1.1. Android ID: A-32769670. **REFERENCE: CVE-2017-0408** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/427 |
| Denial of Service | 08-02-2017 | 7.8 | A denial of service vulnerability in Bionic DNS could enable a remote attacker to use a specially crafted network packet to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32322088. **REFERENCE: CVE-2017-0422** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/428 |
| Execute Code | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as Moderate because it is mitigated by current platform configurations. Product: Android. Versions: N/A. Android ID: | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/429 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | A-32917432.<br>**REFERENCE: CVE-2017-0450** | | |
| Execute Code; Gain Privileges | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32220769.<br>**REFERENCE: CVE-2017-0419** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/430 |
| Execute Code; Gain Privileges | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32703959.<br>**REFERENCE: CVE-2017-0418** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/431 |
| Execute Code; Gain Privileges | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in | https://source.android.com/se | O-GOO-ANDRO- |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32705438. **REFERENCE: CVE-2017-0417** | curity/bulletin/01-02-2017.html | 280217/432 |
| Execute Code; Gain Privileges | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32886609. **REFERENCE: CVE-2017-0416** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/433 |
| Execute Code; Gain Privileges | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in Mediaserver could enable a local malicious application to execute arbitrary code within the context of a privileged | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/434 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32706020. **REFERENCE: CVE-2017-0415** | | |
| Execute Code; Gain Privileges | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in the Framework APIs could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-33039926. **REFERENCE: CVE-2017-0412** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/435 |
| Execute Code; Gain Privileges | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in the Framework APIs could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/436 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | Android. Versions: 7.0, 7.1.1. Android ID: A-33042690. **REFERENCE: CVE-2017-0411** | | |
| Execute Code; Gain Privileges | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in the Framework APIs could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-31929765. **REFERENCE: CVE-2017-0410** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/437 |
| Execute Code; Overflow; Memory Corruption | 08-02-2017 | 9.3 | A remote code execution vulnerability in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. This affects the libhevc library. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32873375. **REFERENCE: CVE-2017-0407** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/438 |
| Execute Code; Overflow; | 08-02-2017 | 9.3 | A remote code execution vulnerability in | https://source.android.com/se | O-GOO-ANDRO- |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| Memory Corruption | | | Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. This affects the libhevc library. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32915871. **REFERENCE: CVE-2017-0406** | curity/bulletin/01-02-2017.html | 280217/439 |
| Execute Code; Overflow; Memory Corruption | 08-02-2017 | 9.3 | A remote code execution vulnerability in Surfaceflinger could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Surfaceflinger process. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-31960359. **REFERENCE: CVE-2017-0405** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/440 |
| Execute Code | 08-02-2017 | 10 | A remote code execution vulnerability in the Qualcomm crypto driver could enable a remote attacker to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of remote code execution in | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/441 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | the context of the kernel. Product: Android. Versions: N/A. Android ID: A-32652894. References: QC-CR#1077457. **REFERENCE: CVE-2016-8418** | | |
| **Google ; Linux** | | | | | |
| ***Android / Linux Kernel***<br>Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets/ The Linux kernel is a monolithic Unix-like computer operating system kernel. | | | | | |
| Gain Information | 08-02-2017 | 2.6 | An information disclosure vulnerability in the Qualcomm sound driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31796345. References: QC-CR#1073129. **REFERENCE: CVE-2017-0451** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/442 |
| Gain Information | 08-02-2017 | 2.6 | An information disclosure vulnerability in the Qualcomm Secure Execution Environment Communicator could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31704078. References: | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/443 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | QC-CR#1076407.<br>**REFERENCE: CVE-2016-8414** | | |
| Gain Information | 08-02-2017 | 4.3 | An information disclosure vulnerability in the NVIDIA video driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it could be used to access sensitive data without explicit user permission. Product: Android. Versions: Kernel-3.10. Android ID: A-32721029. References: N-REFERENCE: CVE-2017-0448.<br>**REFERENCE: CVE-2017-0448** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/444 |
| Gain Privileges; Bypass | 07-02-2017 | 7.2 | The aio_mount function in fs/aio.c in the Linux kernel before 4.7.7 does not properly restrict execute access, which makes it easier for local users to bypass intended SELinux W^X policy restrictions, and consequently gain privileges, via an io_setup system call.<br>**REFERENCE: CVE-2016-10044** | https://github.com/torvalds/linux/commit/22f6b4d34fcf039c63a94e7670e0da24f8575a5a | O-GOO-ANDRO-280217/445 |
| Denial of Service; Gain Privileges | 07-02-2017 | 7.2 | Race condition in the ip4_datagram_release_cb function in net/ipv4/datagram.c in the Linux kernel before 3.15.2 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging incorrect expectations about locking during | https://github.com/torvalds/linux/commit/9709674e68646cee5a24e3000b3558d25412203a | O-GOO-ANDRO-280217/446 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | multithreaded access to internal data structures for IPv4 UDP sockets. **REFERENCE: CVE-2014-9914** | | |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Moderate because it first requires compromising a privileged process and is mitigated by current platform configurations. Product: Android. Versions: Kernel-3.10. Android ID: A-31707909. References: B-RB#32094. **REFERENCE: CVE-2017-0449** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/447 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-32919560. **REFERENCE: CVE-2017-0447** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/448 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local malicious application to execute | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/449 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-32917445. **REFERENCE: CVE-2017-0446** | | |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-32769717. **REFERENCE: CVE-2017-0445** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/450 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Realtek sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-32705232. **REFERENCE: CVE-2017-0444** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/451 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local | https://source.android.com/security/bulletin/01-02- | O-GOO-ANDRO-280217/452 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32877494. References: QC-CR#1092497. **REFERENCE: CVE-2017-0443** | 2017.html | |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32871330. References: QC-CR#1092497. **REFERENCE: CVE-2017-0442** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/453 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/454 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | Kernel-3.18. Android ID: A-32872662. References: QC-CR#1095009. **REFERENCE: CVE-2017-0441** | | |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33252788. References: QC-CR#1095770. **REFERENCE: CVE-2017-0440** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/455 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32450647. References: QC-CR#1092059. **REFERENCE: CVE-2017-0439** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/456 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local | https://source.android.com/security/bulletin/01-02- | O-GOO-ANDRO-280217/457 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32402604. References: QC-CR#1092497. **REFERENCE: CVE-2017-0438** | 2017.html | |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32402310. References: QC-CR#1092497. **REFERENCE: CVE-2017-0437** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/458 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/459 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | Kernel-3.18. Android ID: A-32624661. References: QC-CR#1078000. **REFERENCE: CVE-2017-0436** | | |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31906657. References: QC-CR#1078000. **REFERENCE: CVE-2017-0435** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/460 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Synaptics touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the touchscreen chipset. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-33001936. **REFERENCE: CVE-2017-0434** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/461 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Synaptics touchscreen driver could enable a local malicious application to execute arbitrary code | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/462 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | within the context of the touchscreen chipset. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-31913571.<br>**REFERENCE: CVE-2017-0433** | | |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31906415. References: QC-CR#1078000.<br>**REFERENCE: CVE-2016-8481** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/463 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm Secure Execution Environment Communicator driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31804432. References: | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/464 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | QC-CR#1086186. **REFERENCE: CVE-2016-8480** | | |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32879283. References: QC-CR#1091940. **REFERENCE: CVE-2016-8476** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/465 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32451104. References: QC-CR#1087797. **REFERENCE: CVE-2016-8421** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/466 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/467 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32451171. References: QC-CR#1087807. **REFERENCE: CVE-2016-8420** | | |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32454494. References: QC-CR#1087209. **REFERENCE: CVE-2016-8419** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/468 |
| Execute Code | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/469 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32838767. References: B-RB#107459. **REFERENCE: CVE-2017-0430** | | |
| Execute Code | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-32636619. References: N-REFERENCE: CVE-2017-0429. **REFERENCE: CVE-2017-0429** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/470 |
| Execute Code | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-32401526. References: N- | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/471 |

| CV Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | REFERENCE: CVE-2017-0428. **REFERENCE: CVE-2017-0428** | | |
| Execute Code | 08-02-2017 | 9.3 | An elevation of privilege vulnerability in the kernel file system could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31495866. **REFERENCE: CVE-2017-0427** | https://source.android.com/security/bulletin/01-02-2017.html | O-GOO-ANDRO-280217/472 |
| **Honeywell** | | | | | |
| ***Xl Web II Controller***<br>Excel Web II is Honeywell's Ethernet-based, freely- programmable Building Automation controller offering a combination of BACnet IP, BACnet MS/TP, and LONWORKS communication. It demonstrates Honeywell's full commitment to reducing total installed cost and total building lifecycle cost for building investors and building operators. | | | | | |
| NA | 13-02-2017 | 5 | An issue was discovered in Honeywell XL Web II controller XL1000C500 XLWebExe-2-01-00 and prior, and XLWeb 500 XLWebExe-1-02-08 and prior. Password is stored in clear text. **REFERENCE: CVE-2017-5140** | NA | O-HON-XL WE-280217/473 |
| NA | 13-02-2017 | 5 | An issue was discovered in Honeywell XL Web II controller XL1000C500 XLWebExe-2-01-00 and prior, and XLWeb 500 XLWebExe-1-02-08 and | NA | O-HON-XL WE-280217/474 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | prior. Any user is able to disclose a password by accessing a specific URL, because of Plaintext Storage of a Password. **REFERENCE: CVE-2017-5139** | | |
| NA | 13-02-2017 | 6.5 | An issue was discovered in Honeywell XL Web II controller XL1000C500 XLWebExe-2-01-00 and prior, and XLWeb 500 XLWebExe-1-02-08 and prior. A user with low privileges is able to open and change the parameters by accessing a specific URL because of Improper Privilege Management. **REFERENCE: CVE-2017-5142** | NA | O-HON-XL WE-280217/475 |
| NA | 13-02-2017 | 6.5 | An issue was discovered in Honeywell XL Web II controller XL1000C500 XLWebExe-2-01-00 and prior, and XLWeb 500 XLWebExe-1-02-08 and prior. An attacker can establish a new user session, without invalidating any existing session identifier, which gives the opportunity to steal authenticated sessions (SESSION FIXATION). **REFERENCE: CVE-2017-5141** | NA | O-HON-XL WE-280217/476 |
| Directory Traversal | 13-02-2017 | 7.5 | An issue was discovered in Honeywell XL Web II controller XL1000C500 XLWebExe-2-01-00 and prior, and XLWeb 500 XLWebExe-1-02-08 and | NA | O-HON-XL WE-280217/477 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | prior. A user without authenticating can make a directory traversal attack by accessing a specific URL.<br>**REFERENCE: CVE-2017-5143** | | |
| **IBM** | | | | | |
| ***AIX***<br>AIX is an open operating system from IBM that is based on a version of UNIX. | | | | | |
| NA | 15-02-2017 | 4.9 | IBM AIX 7.1 and 7.2 allows a local user to open a file with a specially crafted argument that would crash the system. IBM APARs: IV91488, IV91487, IV91456, IV90234.<br>**REFERENCE: CVE-2016-8944** | http://aix.software.ibm.com/aix/efixes/security/sysproc_advisory.asc | O-IBM-AIX-280217/478 |
| NA | 01-02-2017 | 7.2 | IBM AIX contains an unspecified vulnerability that would allow a locally authenticated user to obtain root level privileges.<br>**REFERENCE: CVE-2016-3053** | http://aix.software.ibm.com/aix/efixes/security/lsmcode_advisory2.asc | O-IBM-AIX-280217/479 |
| Gain Privileges | 02-02-2017 | 7.2 | IBM AIX 6.1, 7.1, and 7.2 could allow a local user to exploit a vulnerability in the bellmail binary to gain root privileges.<br>**REFERENCE: CVE-2017-1093** | http://aix.software.ibm.com/aix/efixes/security/bellmail_advisory2.asc | O-IBM-AIX-280217/480 |
| ***AIX; Vios***<br>AIX is an open operating system from IBM that is based on a version of UNIX; The Virtual I/O Server facilitates the sharing of physical I/O resources among client logical partitions within the server. | | | | | |
| Gain Privileges | 15-02-2017 | 7.2 | IBM AIX 6.1, 7.1, and 7.2 could allow a local user to gain root privileges using a specially crafted command within the bellmail client. IBM APARs: IV91006, IV91007, | http://aix.software.ibm.com/aix/efixes/security/bellmail_advisory.asc | O-IBM-AIX;V-280217/481 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | IV91008, IV91010, IV91011.<br>**REFERENCE: CVE-2016-8972** | | |
| NA | 15-02-2017 | 7.2 | IBM AIX 5.3, 6.1, 7.1, and 7.2 contains an unspecified vulnerability that would allow a locally authenticated user to obtain root level privileges. IBM APARs: IV88658, IV87981, IV88419, IV87640, IV88053.<br>**REFERENCE: CVE-2016-6079** | http://aix.software.ibm.com/aix/efixes/security/lquerylv_advisory.asc | O-IBM-AIX;V-280217/482 |
| ***Security Access Manager 9.0 Firmware; Security Access Manager For Mobile 8.0 Firmware; Security Access Manager For Web 7.0 Firmware; Security Access Manager For Web 8.0 Firmware***<br>IBM Security Access Manager enables businesses to more securely adopt web, mobile, and cloud technologies and simplifies user access management for employees and consumers. | | | | | |
| NA | 01-02-2017 | 3.5 | IBM Security Access Manager for Web processes patches, image backups and other updates without sufficiently verifying the origin and integrity of the code, which could allow an authenticated attacker to load malicious code.<br>**REFERENCE: CVE-2016-3016** | http://www.ibm.com/support/docview.wss?uid=swg21995518 | O-IBM-SECUR-280217/483 |
| NA | 01-02-2017 | 4 | IBM Security Access Manager for Web could allow an authenticated user to gain access to highly sensitive information due to incorrect file permissions.<br>**REFERENCE: CVE-2016-3022** | http://www.ibm.com/support/docview.wss?uid=swg21995360 | O-IBM-SECUR-280217/484 |
| Gain Information | 01-02-2017 | 4 | IBM Security Access Manager for Web could allow an authenticated attacker to obtain | http://www.ibm.com/support/docview.wss?uid=swg2199543 | O-IBM-SECUR-280217/485 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | sensitive information from error message using a specially crafted HTTP request.<br>**REFERENCE: CVE-2016-3021** | 6 | |
| Gain Information | 01-02-2017 | 5 | IBM Security Access Manager for Web could allow an unauthenticated user to gain access to sensitive information by entering invalid file names.<br>**REFERENCE: CVE-2016-3023** | http://www.ibm.com/support/docview.wss?uid=swg21995348 | O-IBM-SECUR-280217/486 |
| Gain Information | 01-02-2017 | 5 | IBM Security Access Manager for Web could allow a remote attacker to obtain sensitive information due to security misconfigurations.<br>**REFERENCE: CVE-2016-3017** | http://www.ibm.com/support/docview.wss?uid=swg21995519 | O-IBM-SECUR-280217/487 |
| Gain Information | 01-02-2017 | 2.1 | IBM Security Access Manager for Web allows web pages to be stored locally which can be read by another user on the system.<br>**REFERENCE: CVE-2016-3024** | http://www.ibm.com/support/docview.wss?uid=swg21995340 | O-IBM-SECUR-280217/488 |
| Denial of Service | 01-02-2017 | 5.5 | IBM Security Access Manager for Web is vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources. | http://www.ibm.com/support/docview.wss?uid=swg21994440 | O-IBM-SECUR-280217/489 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | **REFERENCE: CVE-2016-3027** | | |
| Denial of Service; Gain Information | 01-02-2017 | 6.4 | IBM Single Sign On for Bluemix could allow a remote attacker to obtain sensitive information, caused by a XML external entity (XXE) error when processing XML data by the XML parser. A remote attacker could exploit this vulnerability to read arbitrary files on the system or cause a denial of service.<br>**REFERENCE: CVE-2016-2908** | http://www.ibm.com/support/docview.wss?uid=swg21995531 | O-IBM-SECUR-280217/490 |
| Cross Site Request Forgery | 01-02-2017 | 6.8 | IBM Security Access Manager for Web is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.<br>**REFERENCE: CVE-2016-3029** | http://www.ibm.com/support/docview.wss?uid=swg21995345 | O-IBM-SECUR-280217/491 |
| **Linux** | | | | | |
| ***Linux Kernel***<br>The Linux kernel is a monolithic Unix-like computer operating system kernel. | | | | | |
| Gain Information | 06-02-2017 | 2.1 | Off-by-one error in the pipe_advance function in lib/iov_iter.c in the Linux kernel before 4.9.5 allows local users to obtain sensitive information from uninitialized heap-memory locations in opportunistic circumstances by reading from a pipe after an incorrect buffer-release decision.<br>**REFERENCE: CVE-2017-** | https://github.com/torvalds/linux/commit/b9dc6f65bc5e232d1c05fe34b5daadc7e8bbf1fb | O-LIN-LINUX-280217/492 |

| CV Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | **5550** | | |
| Gain Information | 06-02-2017 | 2.1 | The klsi_105_get_line_state function in drivers/usb/serial/kl5kusb105.c in the Linux kernel before 4.9.5 places uninitialized heap-memory contents into a log entry upon a failure to read the line status, which allows local users to obtain sensitive information by reading the log.<br>**REFERENCE: CVE-2017-5549** | https://bugzilla.redhat.com/show_bug.cgi?id=1416114 | O-LIN-LINUX-280217/493 |
| Gain Information | 14-02-2017 | 2.1 | The time subsystem in the Linux kernel through 4.9.9, when CONFIG_TIMER_STATS is enabled, allows local users to discover real PID values (as distinguished from PID values inside a PID namespace) by reading the /proc/timer_list file, related to the print_timer function in kernel/time/timer_list.c and the __timer_stats_timer_set_start_info function in kernel/time/timer.c.<br>**REFERENCE: CVE-2017-5967** | http://git.kernel.org/cgit/linux/kernel/git/tip/tip.git/commit/?id=dfb4357da6ddbdf57d583ba64361c9d792b0e0b1 | O-LIN-LINUX-280217/494 |
| Gain Privileges | 06-02-2017 | 3.6 | The simple_set_acl function in fs/posix_acl.c in the Linux kernel before 4.9.6 preserves the setgid bit during a setxattr call involving a tmpfs filesystem, which allows local users to gain group privileges by leveraging | https://github.com/torvalds/linux/commit/497de07d89c1410d76a15bec2bb41f24a2a89f31 | O-LIN-LINUX-280217/495 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | the existence of a setgid program with restrictions on execute permissions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-7097. **REFERENCE: CVE-2017-5551** | | |
| Denial of Service; Gain Privileges | 06-02-2017 | 4.6 | The load_segment_descriptor implementation in arch/x86/kvm/emulate.c in the Linux kernel before 4.9.5 improperly emulates a "MOV SS, NULL selector" instruction, which allows guest OS users to cause a denial of service (guest OS crash) or gain guest OS privileges via a crafted application. **REFERENCE: CVE-2017-2583** | https://bugzilla.redhat.com/show_bug.cgi?id=1414735 | O-LIN-LINUX-280217/496 |
| Denial of Service; Overflow | 06-02-2017 | 4.9 | The vc4_get_bcl function in drivers/gpu/drm/vc4/vc4_gem.c in the VideoCore DRM driver in the Linux kernel before 4.9.7 does not set an errno value upon certain overflow detections, which allows local users to cause a denial of service (incorrect pointer dereference and OOPS) via inconsistent size values in a VC4_SUBMIT_CL ioctl call. **REFERENCE: CVE-2017-5577** | https://bugzilla.redhat.com/show_bug.cgi?id=1416437 | O-LIN-LINUX-280217/497 |
| Denial of Service | 06-02-2017 | 4.9 | The nested_vmx_check_vmptr function in arch/x86/kvm/vmx.c in | https://bugzilla.redhat.com/show_bug.cgi?id=1417812 | O-LIN-LINUX-280217/498 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | the Linux kernel through 4.9.8 improperly emulates the VMXON instruction, which allows KVM L1 guest OS users to cause a denial of service (host OS memory consumption) by leveraging the mishandling of page references.<br>**REFERENCE: CVE-2017-2596** | | |
| Denial of Service | 06-02-2017 | 4.9 | The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.9.8 does not properly validate meta block groups, which allows physically proximate attackers to cause a denial of service (out-of-bounds read and system crash) via a crafted ext4 image.<br>**REFERENCE: CVE-2016-10208** | https://bugzilla.redhat.com/show_bug.cgi?id=1395190 | O-LIN-LINUX-280217/499 |
| Denial of Service; Overflow; Memory Corruption | 06-02-2017 | 4.9 | The smbhash function in fs/cifs/smbencrypt.c in the Linux kernel 4.9.x before 4.9.1 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a scatterlist.<br>**REFERENCE: CVE-2016-10154** | https://github.com/torvalds/linux/commit/06deeec77a5a689cc94b21a8a91a76e42176685d | O-LIN-LINUX-280217/500 |
| Denial of Service | 06-02-2017 | 4.9 | include/linux/init_task.h in the Linux kernel before | https://github.com/torvalds/li | O-LIN-LINUX- |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | 2.6.35 does not prevent signals with a process group ID of zero from reaching the swapper process, which allows local users to cause a denial of service (system crash) by leveraging access to this process group.<br>**REFERENCE: CVE-2010-5328** | nux/commit/fa2755e20ab0c7215d99c2dc7c262e98a09b01df | 280217/501 |
| Denial of Service | 14-02-2017 | 5 | The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a denial of service (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP options.<br>**REFERENCE: CVE-2017-5970** | https://patchwork.ozlabs.org/patch/724136/ | O-LIN-LINUX-280217/502 |
| Denial of Service; Overflow | 06-02-2017 | 7.2 | Integer overflow in the vc4_get_bcl function in drivers/gpu/drm/vc4/vc4_gem.c in the VideoCore DRM driver in the Linux kernel before 4.9.7 allows local users to cause a denial of service or possibly have unspecified other impact via a crafted size value in a VC4_SUBMIT_CL ioctl call.<br>**REFERENCE: CVE-2017-5576** | https://bugzilla.redhat.com/show_bug.cgi?id=1416436 | O-LIN-LINUX-280217/503 |
| Denial of Service; Memory Corruption | 06-02-2017 | 7.2 | drivers/net/ieee802154/atusb.c in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local | http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=05a974efa4bdf6e | O-LIN-LINUX-280217/504 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |

| | | | | | |
|---|---|---|---|---|---|
| | | | users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.<br>**REFERENCE: CVE-2017-5548** | 2a150e3f27dc6fcf0a9ad5655 | |
| Denial of Service; Memory Corruption | 06-02-2017 | 7.2 | drivers/hid/hid-corsair.c in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.<br>**REFERENCE: CVE-2017-5547** | https://github.com/torvalds/linux/commit/6d104af38b570d37aa32a5803b04c354f8ed513d | O-LIN-LINUX-280217/505 |
| Denial of Service | 06-02-2017 | 7.2 | The freelist-randomization feature in mm/slab.c in the Linux kernel 4.8.x and 4.9.x before 4.9.5 allows local users to cause a denial of service (duplicate freelist entries and system crash) or possibly have unspecified other impact in opportunistic circumstances by leveraging the selection of a large value for a random number.<br>**REFERENCE: CVE-2017-5546** | https://github.com/torvalds/linux/commit/c4e490cf148e85ead0d1b1c2caaba833f1d5b29f | O-LIN-LINUX-280217/506 |
| Denial of Service; | 06-02-2017 | 7.2 | The crypto scatterlist API in the Linux kernel 4.9.x | https://github.com/torvalds/li | O-LIN-LINUX- |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Memory Corruption | | | before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging reliance on earlier net/ceph/crypto.c code. **REFERENCE: CVE-2016-10153** | nux/commit/a45f795c65b479b4ba107b6ccde29b896d51ee98 | 280217/507 |
| Execute Code | 08-02-2017 | 7.6 | An elevation of privilege vulnerability in the MediaTek driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-28332719. **REFERENCE: CVE-2017-0432** | https://source.android.com/security/bulletin/01-02-2017.html | O-LIN-LINUX-280217/508 |
| Denial of Service; Gain Privileges | 06-02-2017 | 10 | Use-after-free vulnerability in the kvm_ioctl_create_device function in virt/kvm/kvm_main.c in the Linux kernel before 4.8.13 allows host OS users to cause a denial of service (host OS crash) or possibly gain privileges via crafted ioctl calls on the /dev/kvm device. **REFERENCE: CVE-2016-10150** | https://github.com/torvalds/linux/commit/a0f1d21c1ccb1da66629627a74059dd7f5ac9c61 | O-LIN-LINUX-280217/509 |
| **Moxa** | | | | | |
| ***Edr-810 Firmware***<br>The EDR-810 is a highly integrated industrial multiport secure router with firewall/NAT/VPN and | | | | | |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| managed Layer 2 switch functions. | | | | | |
| NA | 13-02-2017 | 5 | An issue was discovered in Moxa EDR-810 Industrial Secure Router. By accessing a specific uniform resource locator (URL) on the web server, a malicious user is able to access configuration and log files (PRIVILEGE ESCALATION).<br>**REFERENCE: CVE-2016-8346** | NA | O-MOX-EDR-8-280217/510 |
| ***Miineport E1 Firmware; Miineport E2 Firmware; Miineport E3 Firmware***<br>Moxa's MiiNePort embedded device servers are designed for manufacturers who want to add sophisticated network connectivity to their serial devices with minimal integration effort | | | | | |
| NA | 13-02-2017 | 5 | An issue was discovered in Moxa MiiNePort E1 versions prior to 1.8, E2 versions prior to 1.4, and E3 versions prior to 1.1. Configuration data are stored in a file that is not encrypted.<br>**REFERENCE: CVE-2016-9346** | NA | O-MOX-MIINE-280217/511 |
| NA | 13-02-2017 | 5 | An issue was discovered in Moxa MiiNePort E1 versions prior to 1.8, E2 versions prior to 1.4, and E3 versions prior to 1.1. An attacker may be able to brute force an active session cookie to be able to download configuration files.<br>**REFERENCE: CVE-2016-9344** | NA | O-MOX-MIINE-280217/512 |
| **Netapp** | | | | | |
| ***Data Ontap***<br>Clustered Data ONTAP provides up to 24 storage controllers, or nodes, managed as a single logical pool so your operations scale more easily. | | | | | |
| Gain Information | 07-02-2017 | 4.3 | NetApp Data ONTAP before 8.2.4P5, when operating in 7-Mode, | https://kb.netapp.com/support/s/article/NTA | O-NET-DATA -280217/513 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | allows remote attackers to obtain information about the volumes configured for HTTP access. **REFERENCE: CVE-2016-6495** | P-20160929-0001 | |
| Execute Code | 07-02-2017 | 6.5 | NetApp OnCommand System Manager 8.3.x before 8.3.2 allows remote authenticated users to execute arbitrary code via unspecified vectors. **REFERENCE: CVE-2015-8322** | https://kb.netapp.com/support/index?page=content&id=9010070 | O-NET-DATA -280217/514 |
| **Samsung** | | | | | |
| ***Samsung Mobile***<br>Samsung helps you discover a wide range of home electronics with cutting-edge technology including smartphones, tablets, TVs, home appliances and more. | | | | | |
| Denial of Service | 13-02-2017 | 2.1 | Samsung devices with Android KK(4.4) or L(5.0/5.1) allow local users to cause a denial of service (IAndroidShm service crash) via crafted data in a service call. **REFERENCE: CVE-2016-4546** | http://security.samsungmobile.com/smrupdate.html#SMR-JAN-2016 | O-SAM-SAMSU-280217/515 |
| Denial of Service | 13-02-2017 | 5 | Samsung devices with Android KK(4.4), L(5.0/5.1), or M(6.0) allow attackers to cause a denial of service (system crash) via a crafted system call to TvoutService_C. **REFERENCE: CVE-2016-4547** | http://security.samsungmobile.com/smrupdate.html#SMR-FEB-2016 | O-SAM-SAMSU-280217/516 |
| **Schneider Electric** | | | | | |
| ***Homelynk Controller Lss100100 Firmware***<br>NA | | | | | |
| Execute Code; Cross Site Scripting | 13-02-2017 | 4.3 | An issue was discovered in Schneider Electric homeLYnk Controller, LSS100100, all versions prior to V1.5.0. The homeLYnk controller is | NA | O-SCH-HOMEL-280217/517 |

| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | susceptible to a cross-site scripting attack. User inputs can be manipulated to cause execution of JavaScript code.<br>**REFERENCE: CVE-2017-5157** | | |
| **Sendquick** | | | | | |
| ***Avera Sms Gateway Firmware;Entera Sms Gateway Firmware***<br>An SMS gateway allows a computer to send or receive Short Message Service (SMS) transmissions to or from a telecommunications network. | | | | | |
| NA | 05-02-2017 | 5 | An issue was discovered on SendQuick Entera and Avera devices before 2HF16. An attacker could request and download the SMS logs from an unauthenticated perspective.<br>**REFERENCE: CVE-2017-5137** | NA | O-SEN-AVERA-280217/518 |
| Execute Code | 05-02-2017 | 7.5 | An issue was discovered on SendQuick Entera and Avera devices before 2HF16. Multiple Command Injection vulnerabilities allow attackers to execute arbitrary system commands.<br>**REFERENCE: CVE-2016-10098** | NA | O-SEN-AVERA-280217/519 |
| NA | 05-02-2017 | 7.8 | An issue was discovered on SendQuick Entera and Avera devices before 2HF16. The application failed to check the access control of the request which could result in an attacker being able to shutdown the system.<br>**REFERENCE: CVE-2017-5136** | NA | O-SEN-AVERA-280217/520 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **CV Scoring Scale** | **0-1** | **1-2** | **2-3** | **3-4** | **4-5** | **5-6** | **6-7** | **7-8** | **8-9** | **9-10** |