| Vulnerability Type(s) | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Application** | | | | | |
| **Artifex** | | | | | |
| ***Mupdf*** | | | | | |
| DoS | 02-02-2018 | 4.3 | pdf_load_obj_stm in pdf/pdf-xref.c in Artifex MuPDF 1.12.0 could reference the object stream recursively and therefore run out of error stack, which allows remote attackers to cause a denial of service via a crafted PDF document. **CVE ID : CVE-2018-6544** | NA | A-ART-MUPDF-160218/1 |
| **Atlassian** | | | | | |
| ***Bamboo*** | | | | | |
| XSS | 02-02-2018 | 3.5 | The plan configure branches resource in Atlassian Bamboo before version 6.2.3 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability through the name of a branch. **CVE ID : CVE-2017-18082** | https://jira.atlassian.com/browse/BAM-19666 | A-ATL-BAMBO-160218/2 |
| XSS | 02-02-2018 | 3.5 | The viewDeploymentVersionJiraIssuesDialog resource in Atlassian Bamboo before version 6.2.0 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the name of a release. **CVE ID : CVE-2017-18041** | https://jira.atlassian.com/browse/BAM-19662 | A-ATL-BAMBO-160218/3 |
| XSS | 02-02-2018 | 3.5 | The viewDeploymentVersionCommits resource in Atlassian Bamboo before version 6.2.0 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the name of a release. **CVE ID : CVE-2017-18040** | https://jira.atlassian.com/browse/BAM-19661 | A-ATL-BAMBO-160218/4 |
| XSS CSRF | 02-02-2018 | 4.3 | The signupUser resource in Atlassian Bamboo before version 6.3.1 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability through the value of the csrf token cookie. **CVE ID : CVE-2017-18081** | https://jira.atlassian.com/browse/BAM-19665 | A-ATL-BAMBO-160218/5 |
| CSRF | 02-02-2018 | 6.8 | The saveConfigureSecurity resource in Atlassian Bamboo before version 6.3.1 allows remote attackers to modify security settings via a Cross-site request forgery | https://jira.atlassian.com/browse/BAM-19664 | A-ATL-BAMBO-160218/6 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (CSRF) vulnerability.<br>**CVE ID : CVE-2017-18080** | | |
| CSRF | 02-02-2018 | 6.8 | The update user administration resource in Atlassian Bamboo before version 6.3.1 allows remote attackers to modify user data including passwords via a Cross-site request forgery (CSRF) vulnerability.<br>**CVE ID : CVE-2017-18042** | https://jira.atlassian.com/browse/BAM-19663 | A-ATL-BAMBO-160218/7 |
| ***Confluence*** | | | | | |
| XSS | 02-02-2018 | 3.5 | The usermacros resource in Atlassian Confluence Server before version 6.3.4 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability through the description of a macro.<br>**CVE ID : CVE-2017-18084** | https://jira.atlassian.com/browse/CONFSERVER-54904 | A-ATL-CONFL-160218/8 |
| XSS | 02-02-2018 | 3.5 | The editinword resource in Atlassian Confluence Server before version 6.4.0 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability through the contents of an uploaded file.<br>**CVE ID : CVE-2017-18083** | https://jira.atlassian.com/browse/CONFSERVER-54903 | A-ATL-CONFL-160218/9 |
| XSS | 02-02-2018 | 4.3 | Various resources in Atlassian Confluence Server before version 6.4.2 allow remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the issuesURL parameter.<br>**CVE ID : CVE-2017-18086** | https://jira.atlassian.com/browse/CONFSERVER-54907 | A-ATL-CONFL-160218/10 |
| XSS | 02-02-2018 | 4.3 | The viewdefaultdecorator resource in Atlassian Confluence Server before version 6.6.1 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability through the key parameter.<br>**CVE ID : CVE-2017-18085** | https://jira.atlassian.com/browse/CONFSERVER-54905 | A-ATL-CONFL-160218/11 |
| ***Crucible;Fisheye*** | | | | | |
| XSS | 02-02-2018 | 3.5 | The source browse resource in Atlassian FishEye and Crucible before version 4.5.1 and 4.6.0 allows allows remote attackers that have write access to an indexed repository to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in via a specially crafted repository branch name when trying to display deleted files of the branch.<br>**CVE ID : CVE-2017-18034** | https://jira.atlassian.com/browse/FE-6994 | A-ATL-CRUCI-160218/12 |
| NA | 02-02-2018 | 4 | The /rest/review-coverage-chart/1.0/data/<repository_name>/.json resource in Atlassian Fisheye and | https://jira.atlassian.com/browse/CRUC-8163 | A-ATL-CRUCI- |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Crucible before version 4.5.1 and 4.6.0 was missing a permissions check, this allows remote attackers who do not have access to a particular repository to determine its existence and access review coverage statistics for it. **CVE ID : CVE-2017-18035** | | 160218/13 |
| ***Jira*** | | | | | |
| XSS | 02-02-2018 | 4.3 | The IncomingMailServers resource in Atlassian Jira from version 6.2.1 before version 7.4.4 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the messagesThreshold parameter. **CVE ID : CVE-2017-18039** | https://jira.atlassian.com/browse/JRASERVER-66719 | A-ATL-JIRA-160218/14 |
| **Claymore Dual Miner Project** | | | | | |
| ***Claymore Dual Miner*** | | | | | |
| DoS | 02-02-2018 | 6.4 | The remote management interface in Claymore Dual Miner 10.5 and earlier is vulnerable to an unauthenticated format string vulnerability, allowing remote attackers to read memory or cause a denial of service. **CVE ID : CVE-2018-6317** | NA | A-CLA-CLAYM-160218/15 |
| **Dojotoolkit** | | | | | |
| ***Dojo*** | | | | | |
| XSS | 02-02-2018 | 4.3 | dijit.Editor in Dojo Toolkit 1.13 allows XSS via the onload attribute of an SVG element. **CVE ID : CVE-2018-6561** | https://github.com/imsebao/404team/blob/master/dijit_editor_xss.md | A-DOJ-DOJO-160218/16 |
| **Echor Project** | | | | | |
| ***Echor*** | | | | | |
| NA | 02-02-2018 | 4.6 | The perform_request function in /lib/echor/backplane.rb in echor 0.1.6 Ruby Gem allows local users to inject arbitrary code by adding a semi-colon in their username or password. **CVE ID : CVE-2014-1834** | http://www.openwall.com/lists/oss-security/2014/01/31/10 | A-ECH-ECHOR-160218/17 |
| **Evergreen-ils** | | | | | |
| ***Evergreen*** | | | | | |
| Gain Information | 01-02-2018 | 4 | Evergreen 2.5.9, 2.6.7, and 2.7.4 allows remote authenticated users with STAFF_LOGIN permission to obtain sensitive settings history information by leveraging listing of open-ils.pcrud as a controller in the IDL. **CVE ID : CVE-2015-2203** | https://bugs.launchpad.net/evergreen/+bug/1206589 | A-EVE-EVERG-160218/18 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Ezcode** | | | | | |
| ***Event Manager*** | | | | | |
| Sql | 02-02-2018 | 7.5 | SQL Injection exists in Event Manager 1.0 via the event.php id parameter or the page.php slug parameter. **CVE ID : CVE-2018-6576** | https://www.exploit-db.com/exploits/43949 | A-EZC-EVENT-160218/19 |
| **Flexense** | | | | | |
| ***Diskboss*** | | | | | |
| Gain Information | 02-02-2018 | 4.3 | An issue was discovered in Flexense DiskBoss 8.8.16 and earlier. Due to the usage of plaintext information from the handshake as input for the encryption key used for the encryption of the rest of the session, the server and client disclose sensitive information, such as the authentication credentials, to any man-in-the-middle (MiTM) listener. **CVE ID : CVE-2018-5261** | https://github.com/bitsadmin/exploits/tree/master/ CVE ID : CVE-2018-5261 | A-FLE-DISKB-160218/20 |
| ***Syncbreeze*** | | | | | |
| Execute Code Overflow | 02-02-2018 | 7.5 | A buffer overflow vulnerability in the control protocol of Flexense SyncBreeze Enterprise v10.4.18 allows remote attackers to execute arbitrary code by sending a crafted packet to TCP port 9121. **CVE ID : CVE-2018-6537** | https://www.exploit-db.com/exploits/43936/ | A-FLE-SYNCB-160218/21 |
| **Gifsicle Project** | | | | | |
| ***Gifsicle*** | | | | | |
| NA | 02-02-2018 | 6.8 | A double-free bug in the read_gif function in gifread.c in gifsicle 1.90 allows a remote attacker to cause a denial-of-service attack or unspecified other impact via a maliciously crafted file, because last_name is mishandled, a different vulnerability than CVE ID : CVE-2017-1000421. **CVE ID : CVE-2017-18120** | NA | A-GIF-GIFSI-160218/22 |
| **GNU** | | | | | |
| ***Binutils*** | | | | | |
| DoS Overflow | 02-02-2018 | 6.8 | In GNU Binutils 2.30, there's an integer overflow in the function load_specific_debug_section() in objdump.c, which results in `malloc()` with 0 size. A crafted ELF file allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact. **CVE ID : CVE-2018-6543** | NA | A-GNU-BINUT-160218/23 |
| **IBM** | | | | | |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ***Emptoris Sourcing*** | | | | | |
| NA | 02-02-2018 | 4.9 | Open redirect vulnerability in IBM Emptoris Sourcing 10.0.0.x before 10.0.0.1_iFix3, 10.0.1.x before 10.0.1.3_iFix3, 10.0.2.x before 10.0.2.8_iFix1, 10.0.4.0 before 10.0.4.0_iFix8, and 10.1.0.0 before 10.1.0.0_iFix3 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors. IBM X-Force ID: 111692. **CVE ID : CVE-2016-0329** | http://www-01.ibm.com/support/docview.wss?uid=swg21982629 | A-IBM-EMPTO-160218/24 |
| ***Tivoli Business Service Manager*** | | | | | |
| XSS | 02-02-2018 | 3.5 | Cross-site scripting (XSS) vulnerability in IBM Tivoli Business Service Manager 6.1.0 before 6.1.0-TIV-BSM-FP0004 and 6.1.1 before 6.1.1-TIV-BSM-FP0004 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. IBM X-Force ID: 111480. **CVE ID : CVE-2016-0311** | https://www.ibm.com/blogs/psirt/ibm-security-bulletin-cross-site-scripting-vulnerability-in-tivoli-business-service-manager-CVE ID : CVE-2016-0311/ | A-IBM-TIVOL-160218/25 |
| ***Tivoli Integrated Portal*** | | | | | |
| XSS | 02-02-2018 | 3.5 | Cross-site scripting (XSS) vulnerability in IBM Tivoli Integrated Portal 2.2.0.0 through 2.2.0.15 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE ID : CVE-2016-0303** | http://www-01.ibm.com/support/docview.wss?uid=swg21981591 | A-IBM-TIVOL-160218/26 |
| ***Tririga Application Platform*** | | | | | |
| Gain Information | 02-02-2018 | 5 | IBM TRIRIGA Application Platform before 3.3.2 allows remote attackers to obtain sensitive information via vectors related to granting unauthenticated access to Document Manager. IBM X-Force ID: 111486. **CVE ID : CVE-2016-0312** | http://www-01.ibm.com/support/docview.wss?uid=swg21979762 | A-IBM-TRIRI-160218/27 |
| NA | 02-02-2018 | 5.5 | IBM TRIRIGA Application Platform 3.3 before 3.3.2.6, 3.4 before 3.4.2.3, and 3.5 before 3.5.0.1 allows remote authenticated users to read or modify arbitrary reports by leveraging an incorrect grant of access. IBM X-Force ID: 111783. **CVE ID : CVE-2016-0342** | http://www-01.ibm.com/support/docview.wss?uid=swg21980252 | A-IBM-TRIRI-160218/28 |
| NA | 02-02-2018 | 5.5 | IBM TRIRIGA Application Platform 3.3 before 3.3.2.6, 3.4 before 3.4.2.3, and 3.5 before 3.5.0.1 might allow remote attackers to access arbitrary JSP pages via vectors related to improper input | http://www-01.ibm.com/support/docview.wss?uid=swg21979760 | A-IBM-TRIRI-160218/29 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | validation. IBM X-Force ID: 111412. **CVE ID : CVE-2016-0300** | | |
| **Inca** | | | | | |
| ***Nprotect Avs*** | | | | | |
| DoS | 01-02-2018 | 6.1 | In nProtect AVS V4.0 before 4.0.0.39, the driver file (TKFsAv.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x220458. **CVE ID : CVE-2018-6525** | http://inca.co.kr/include_file/pdf_down/nProtect%20AVS%20V4%20Vulnerability%20Response%20Release%20Notes.pdf | A-INC-NPROT-160218/30 |
| DoS | 01-02-2018 | 6.1 | In nProtect AVS V4.0 before 4.0.0.39, the driver file (TKFsAv.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x220c20. **CVE ID : CVE-2018-6524** | http://inca.co.kr/include_file/pdf_down/nProtect%20AVS%20V4%20Vulnerability%20Response%20Release%20Notes.pdf | A-INC-NPROT-160218/31 |
| DoS | 01-02-2018 | 6.1 | In nProtect AVS V4.0 before 4.0.0.39, the driver file (TKFsAv.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x22045c. **CVE ID : CVE-2018-6523** | http://inca.co.kr/include_file/pdf_down/nProtect%20AVS%20V4%20Vulnerability%20Response%20Release%20Notes.pdf | A-INC-NPROT-160218/32 |
| DoS | 01-02-2018 | 6.1 | In nProtect AVS V4.0 before 4.0.0.39, the driver file (TKRgFtXp.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x220408. **CVE ID : CVE-2018-6522** | http://inca.co.kr/include_file/pdf_down/nProtect%20AVS%20V4%20Vulnerability%20Response%20Release%20Notes.pdf | A-INC-NPROT-160218/33 |
| **Intel** | | | | | |
| ***Graphics Driver*** | | | | | |
| NA | 02-02-2018 | 7.2 | Pointer dereference in subsystem in Intel Graphics Driver 15.40.x.x, 15.45.x.x, 15.46.x.x allows unprivileged user to elevate privileges via local access. **CVE ID : CVE-2017-5727** | https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00089&languageid=en-fr | A-INT-GRAPH-160218/34 |
| **Ipswitch** | | | | | |
| ***Moveit*** | | | | | |
| XSS | 02-02-2018 | 4.3 | Ipswitch MoveIt v8.1 is vulnerable to a Stored Cross-Site Scripting (XSS) vulnerability, as demonstrated by | https://crowdshield.com/blog.php?name=ipswitc | A-IPS-MOVEI-160218/ |

| Vulnerability Type(s) | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | human.aspx. Attackers can leverage this vulnerability to send malicious messages to other users in order to steal session cookies and launch client-side attacks. **CVE ID : CVE-2018-6545** | h-moveit-stored-xss | 35 |
| **Janguo** | | | | | |
| ***Jimtawl*** | | | | | |
| NA | 02-02-2018 | 7.5 | Arbitrary file upload exists in the Jimtawl 2.1.6 and 2.2.5 component for Joomla! via a view=upload&task=upload&pop=true&tmpl=component request. **CVE ID : CVE-2018-6580** | https://www.exploit-db.com/exploits/43958 | A-JAN-JIMTA-160218/36 |
| **Jextn** | | | | | |
| ***Classified*** | | | | | |
| Sql | 02-02-2018 | 7.5 | SQL Injection exists in the JEXTN Classified 1.0.0 component for Joomla! via a view=boutique&sid= request. **CVE ID : CVE-2018-6575** | https://www.exploit-db.com/exploits/43957 | A-JEX-CLASS-160218/37 |
| ***Je Paypervideo*** | | | | | |
| Sql | 02-02-2018 | 7.5 | SQL Injection exists in the JE PayperVideo 3.0.0 component for Joomla! via the usr_plan parameter in a view=myplans&task=myplans.usersubscriptions request.**CVE ID : CVE-2018-6578** | https://www.exploit-db.com/exploits/43948 | A-JEX-JEPA-160218/38 |
| ***Membership*** | | | | | |
| Sql | 02-02-2018 | 7.5 | SQL Injection exists in the JEXTN Membership 3.1.0 component for Joomla! via the usr_plan parameter in a view=myplans&task=myplans.usersubscriptions request.**CVE ID : CVE-2018-6577** | https://www.exploit-db.com/exploits/43940 | A-JEX-MEMBE-160218/39 |
| ***Reverse Auction*** | | | | | |
| Sql | 02-02-2018 | 7.5 | SQL Injection exists in the JEXTN Reverse Auction 3.1.0 component for Joomla! via a view=products&uid= request. **CVE ID : CVE-2018-6579** | https://www.exploit-db.com/exploits/43950 | A-JEX-REVER-160218/40 |
| **Joommasters** | | | | | |
| ***Jms Music*** | | | | | |
| Sql | 02-02-2018 | 7.5 | SQL Injection exists in the JMS Music 1.1.1 component for Joomla! via a search with the keyword, artist, or username parameter. **CVE ID : CVE-2018-6581** | https://www.exploit-db.com/exploits/43959 | A-JOO-JMSM-160218/41 |
| **Kkcald Project** | | | | | |
| ***Kkcald*** | | | | | |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| XSS | 01-02-2018 | 4.3 | Cross-site scripting vulnerability in epg search result viewer (kkcald) 0.7.21 and earlier allows an attacker to inject arbitrary web script or HTML via unspecified vectors. **CVE ID : CVE-2018-0508** | http://dbit.web.fc2.com/ | A-KKC-KKCAL-160218/42 |
| CSRF | 01-02-2018 | 6.8 | Cross-site request forgery (CSRF) vulnerability in epg search result viewer (kkcald) 0.7.21 and earlier allows an attacker to hijack the authentication of administrators via unspecified vectors. **CVE ID : CVE-2018-0509** | http://dbit.web.fc2.com/ | A-KKC-KKCAL-160218/43 |
| DoS Overflow | 01-02-2018 | 7.5 | Buffer overflow in epg search result viewer (kkcald) 0.7.19 and earlier allows remote attackers to perform unintended operations or execute DoS (denial of service) attacks via unspecified vectors. **CVE ID : CVE-2018-0510** | http://dbit.web.fc2.com/ | A-KKC-KKCAL-160218/44 |
| **Monstra** | | | | | |
| ***Monstra*** | | | | | |
| XSS | 02-02-2018 | 3.5 | Monstra CMS through 3.0.4 has XSS in the title function in plugins/box/pages/pages.plugin.php via a page title to admin/index.php. **CVE ID : CVE-2018-6550** | https://github.com/monstra-cms/monstra/commit/388ab412035474068758df6b07e7e06852f3747b | A-MON-MONST-160218/45 |
| **Nibbleblog** | | | | | |
| ***Nibbleblog*** | | | | | |
| Gain Information | 01-02-2018 | 5 | Nibbleblog 4.0.5 on macOS defaults to having .DS_Store in each directory, causing DS_Store information to leak. **CVE ID : CVE-2018-6470** | https://github.com/dignajar/nibbleblog/issues/120 | A-NIB-NIBBL-160218/46 |
| **Projectpier Project** | | | | | |
| ***Projectpier*** | | | | | |
| XSS | 02-02-2018 | 4.3 | Multiple cross-site scripting (XSS) vulnerabilities in Project-Pier ProjectPier-Core allow remote attackers to inject arbitrary web script or HTML via the search_for parameter to (1) search_by_tag.php, (2) search_contacts.php, or (3) search.php. **CVE ID : CVE-2015-2796** | https://github.com/Project-Pier/ProjectPier-Core/commit/74ecbd4e939a65ba643a4af05fbdb1bb66992435 | A-PRO-PROJE-160218/47 |
| **Sophos** | | | | | |
| ***Sophos Tester*** | | | | | |
| DoS | 02-02-2018 | 4.9 | In Sophos Tester Tool 3.2.0.7 Beta, the driver accepts a special DeviceIoControl code that doesn't check its argument. This | https://29wspy.ru/exploits/CVE ID : CVE-2018- | A-SOP-SOPHO- |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | argument is a memory address: if a caller passes a NULL pointer or a random invalid address, the driver will cause a Blue Screen of Death. If a program or malware does this at boot time, it can cause a persistent denial of service on the machine. **CVE ID : CVE-2018-6319** | 6319.pdf | 160218/48 |
| NA | 02-02-2018 | 9.3 | In Sophos Tester Tool 3.2.0.7 Beta, the driver loads (in the context of the application used to test an exploit or ransomware) the DLL using a payload that runs from NTDLL.DLL (so, it's run in userland), but the driver doesn't perform any validation of this DLL (not its signature, not its hash, etc.). A person can change this DLL in a local way, or with a remote connection, to a malicious DLL with the same name -- and when the product is used, this malicious DLL will be loaded, aka a DLL Hijacking attack. **CVE ID : CVE-2018-6318** | https://29wspy.ru/exploits/CVE ID : CVE-2018-6318.pdf | A-SOP-SOPHO-160218/49 |
| **Sugarcrm** | | | | | |
| ***Sugarcrm*** | | | | | |
| Execute Code | 01-02-2018 | 7.5 | XML external entity (XXE) vulnerability in the RSSDashlet dashlet in SugarCRM before 6.5.17 allows remote attackers to read arbitrary files or potentially execute arbitrary code via a crafted DTD in an XML request. **CVE ID : CVE-2014-3244** | NA | A-SUG-SUGAR-160218/50 |
| **Zziplib Project** | | | | | |
| ***Zziplib*** | | | | | |
| DoS | 01-02-2018 | 4.3 | In ZZIPlib 0.13.67, there is a memory alignment error and bus error in the __zzip_fetch_disk_trailer function of zzip/zip.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted zip file. **CVE ID : CVE-2018-6484** | https://github.com/gdraheim/zziplib/issues/14 | A-ZZI-ZZIPL-160218/51 |
| NA | 02-02-2018 | 4.3 | In ZZIPlib 0.13.67, there is a bus error (when handling a disk64_trailer seek value) caused by loading of a misaligned address in the zzip_disk_findfirst function of zzip/mmapped.c. **CVE ID : CVE-2018-6542** | https://github.com/gdraheim/zziplib/issues/17 | A-ZZI-ZZIPL-160218/52 |
| DoS | 02-02-2018 | 4.3 | In ZZIPlib 0.13.67, there is a bus error caused by loading of a misaligned address (when handling disk64_trailer local entries) in __zzip_fetch_disk_trailer (zzip/zip.c). Remote attackers could leverage this vulnerability to cause a | https://github.com/gdraheim/zziplib/issues/16 | A-ZZI-ZZIPL-160218/53 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | denial of service via a crafted zip file. **CVE ID : CVE-2018-6541** | | |
| DoS | 02-02-2018 | 4.3 | In ZZIPlib 0.13.67, there is a bus error caused by loading of a misaligned address in the zzip_disk_findfirst function of zzip/mmapped.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted zip file. **CVE ID : CVE-2018-6540** | https://github.com/gdraheim/zziplib/issues/15 | A-ZZI-ZZIPL-160218/54 |
| **Apport Project/Canonical** | | | | | |
| ***Apport/Ubuntu Linux*** | | | | | |
| DoS privileges | 02-02-2018 | 7.2 | Apport 2.13 through 2.20.7 does not properly handle crashes originating from a PID namespace allowing local users to create certain files as root which an attacker could leverage to perform a denial of service via resource exhaustion or possibly gain root privileges, a different vulnerability than CVE ID : CVE-2017-14179. **CVE ID : CVE-2017-14180** | https://people.canonical.com/~ubuntu-security/cve/?cve=CVE ID : CVE-2017-14180 | A-APP-APPOR-160218/55 |
| DoS privileges | 02-02-2018 | 7.2 | Apport through 2.20.7 does not properly handle core dumps from setuid binaries allowing local users to create certain files as root which an attacker could leverage to perform a denial of service via resource exhaustion or possibly gain root privileges. NOTE: this vulnerability exists because of an incomplete fix for CVE ID : CVE-2015-1324. **CVE ID : CVE-2017-14177** | https://launchpad.net/bugs/1726372 | A-APP-APPOR-160218/56 |
| **OPERATING SYSTEM(OS)** | | | | | |
| **Canonical** | | | | | |
| ***Ubuntu Linux*** | | | | | |
| DoS privileges | 02-02-2018 | 7.2 | Apport before 2.13 does not properly handle crashes originating from a PID namespace allowing local users to create certain files as root which an attacker could leverage to perform a denial of service via resource exhaustion, possibly gain root privileges, or escape from containers. **CVE ID : CVE-2017-14179** | https://launchpad.net/bugs/1726372 | O-CAN-UBUNT-160218/57 |
| **Operating System; Application (OS/A)** | | | | | |
| **Debian/Simplesamlphp** | | | | | |
| ***Debian Linux/Simplesamlphp*** | | | | | |
| Execute Code XSS | 02-02-2018 | 4.3 | The consentAdmin module in SimpleSAMLphp through 1.14.15 is vulnerable to a Cross-Site Scripting attack, allowing an attacker to craft links that could execute arbitrary JavaScript | https://simplesamlphp.org/security/201709-01 | O-DEB-DEBIA-160218/58 |

| Vulnerability Type(s) | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | code on the victim's web browser.<br>**CVE ID : CVE-2017-18121** | | |
| Bypass | 02-02-2018 | 6.8 | A signature-validation bypass issue was discovered in SimpleSAMLphp through 1.14.16. A SimpleSAMLphp Service Provider using SAML 1.1 will regard as valid any unsigned SAML response containing more than one signed assertion, provided that the signature of at least one of the assertions is valid. Attributes contained in all the assertions received will be merged and the entityID of the first assertion received will be used, allowing an attacker to impersonate any user of any IdP given an assertion signed by the targeted IdP.<br>**CVE ID : CVE-2017-18122** | https://simplesamlphp.org/security/201710-01 | O-DEB-DEBIA-160218/59 |