DEPENDENCY-CHECK

How to read the report | Suppressing false positives | Getting Help: google group | github issues

Project: OpenMRS

Scan Information (show all):

- *dependency-check version*: 3.3.1
- *Report Generated On*: Sep 6, 2018 at 23:14:53 -04:00
- *Dependencies Scanned*: 774 (376 unique)
- *Vulnerable Dependencies*: 56
- *Vulnerabilities Found*: 244
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	CPE	Coordinates	Highest Severity	CVE Count	CPE Confidence	Evidence Count
chartsearch-server-2.1.0.jar	cpe:/a:apache:solr:2.1.0	org.openmrs.module:chartsearch-server:2.1.0	High	8	Low	22
hibernate-validator-4.2.0.Final.jar	cpe:/a:hibernate:hibernate_validator:4.2.0	org.hibernate:hibernate-validator:4.2.0.Final ✓	Medium	1	Highest	37
jackson-databind-2.5.4.jar	cpe:/a:fasterxml:jackson-databind:2.5.4 cpe:/a:fasterxml:jackson:2.5.4	com.fasterxml.jackson.core:jackson-databind:2.5.4	High	5	Highest	35
jetty-jmx-8.1.10.v20130312.jar	cpe:/a:eclipse:jetty:8.1.10.v20130312 cpe:/a:jetty:jetty:8.1.10.v20130312	org.eclipse.jetty:jetty-jmx:8.1.10.v20130312	High	4	Low	31
xalan-2.7.0.jar	cpe:/a:apache:xalan-java:2.7.0	xalan:xalan:2.7.0 ✓	High	1	Highest	27
org.restlet-2.1.1.jar	cpe:/a:restlet:restlet_framework:2.1.1 cpe:/a:restlet:restlet:2.1.1		High	5	Highest	7
poi-3.12.jar	cpe:/a:apache:poi:3.12	org.apache.poi:poi:3.12 ✓	High	2	Low	30
xercesImpl-2.8.0.jar	cpe:/a:apache:xerces2_java:2.8.0	xerces:xercesImpl:2.8.0 ✓	High	1	Low	53
registrationapp-api-1.12.0.jar	cpe:/a:app_project:app:1.12.0	org.openmrs.module:registrationapp-api:1.12.0	Medium	1	Low	22
stax-api-1.0.1.jar	cpe:/a:st_project:st:1.0.1	stax:stax-api:1.0.1 ✓	Medium	1	Low	27
jackson-databind-2.8.1.jar	cpe:/a:fasterxml:jackson-databind:2.8.1 cpe:/a:fasterxml:jackson:2.8.1	com.fasterxml.jackson.core:jackson-databind:2.8.1	High	5	Highest	35
activemq-core-5.4.3.jar	cpe:/a:apache:activemq:5.4.3	org.apache.activemq:activemq-core:5.4.3	High	21	Highest	29
appframework-api-2.11.0.jar	cpe:/a:app_project:app:2.11.0	org.openmrs.module:appframework-api:2.11.0	Medium	1	Low	21
formentryapp-api-1.4.2.jar	cpe:/a:app_project:app:1.4.2	org.openmrs.module:formentryapp-api:1.4.2	Medium	1	Low	21
stax-1.2.0.jar	cpe:/a:st_project:st:1.2.0	stax:stax:1.2.0 ✓	Medium	1	Low	27
xstream-1.4.3.jar	cpe:/a:xstream_project:xstream:1.4.3	com.thoughtworks.xstream:xstream:1.4.3	Medium	2	Low	17
kahadb-5.4.3.jar	cpe:/a:apache:activemq:5.4.3	org.apache.activemq:kahadb:5.4.3	High	21	Highest	25
httpclient-4.2.jar	cpe:/a:apache:httpclient:4.2	org.apache.httpcomponents:httpclient:4.2	Medium	1	Highest	28
hadoop-auth-2.2.0.jar	cpe:/a:apache:hadoop:2.2.0	org.apache.hadoop:hadoop-auth:2.2.0	High	7	Highest	22
protobuf-java-2.5.0.jar	cpe:/a:google:protobuf:2.5.0	com.google.protobuf:protobuf-java:2.5.0	Medium	1	Highest	25
commons-beanutils-1.7.0.jar	cpe:/a:apache:commons_beanutils:1.7.0	commons-beanutils:commons-beanutils:1.7.0 ✓	High	1	Low	22
jasypt-1.6.jar	cpe:/a:jasypt_project:jasypt:1.6	org.jasypt:jasypt:1.6	Medium	1	Low	19
mysql-connector-java-5.1.28.jar	cpe:/a:oracle:mysql:5.1.28 cpe:/a:mysql:mysql:5.1.28 cpe:/a:oracle:mysql_connectors:5.1.28 cpe:/a:sun:mysql_connector/j:5.1.28 cpe:/a:oracle:connector/j:5.1.28	mysql:mysql-connector-java:5.1.28 ✓	Medium	4	Highest	36
zookeeper-3.4.6.jar	cpe:/a:apache:zookeeper:3.4.6	org.apache.zookeeper:zookeeper:3.4.6 ✓	Medium	4	Highest	25

Dependency	CPE	Coordinates	Highest Severity	CVE Count	CPE Confidence	Evidence Count
standard-1.1.2.jar	cpe:/a:apache:standard_taglibs:1.1.2	taglibs:standard:1.1.2 ✓	High	1	Low	24
commons-fileupload-1.2.1.jar	cpe:/a:apache:commons_fileupload:1.2.1	commons-fileupload:commons-fileupload:1.2.1	High	4	Highest	27
chartsearch-api-2.1.0.jar	cpe:/a:openmrs:openmrs:2.1::~~standalone~~~	org.openmrs.module:chartsearch-api:2.1.0	High	4	Highest	21
serialization.xstream-api-0.2.14.jar	cpe:/a:xstream_project:xstream:0.2.14	org.openmrs.module:serialization.xstream-api:0.2.14	Medium	2	Low	22
ognl-3.0.8.jar	cpe:/a:ognl_project:ognl:3.0.8	ognl:ognl:3.0.8	Medium	1	Low	19
solr-core-4.10.4.jar	cpe:/a:apache:solr:4.10.4	org.apache.solr:solr-core:4.10.4 ✓	Medium	4	Low	28
mysql.exe	cpe:/a:mysql:mysql:-		High	25	Low	2
dwr-2.0.7-mod.jar	cpe:/a:directwebremoting:direct_web_remoting:2.0.7 cpe:/a:getahead:direct_web_remoting:2.0.7 cpe:/a:openmrs:openmrs:2.0.7	org.openmrs.directwebremoting:dwr:2.0.5-mod	Medium	2	Low	16
activeio-core-3.1.2.jar	cpe:/a:apache:activemq:3.1.2	org.apache.activemq:activeio-core:3.1.2	High	14	Low	25
struts-core-1.3.8.jar	cpe:/a:apache:struts:1.3.8	org.apache.struts:struts-core:1.3.8	High	4	Highest	22
struts-tiles-1.3.8.jar	cpe:/a:apache:struts:1.3.8 cpe:/a:apache:tiles:1.3.8	org.apache.struts:struts-tiles:1.3.8	High	4	Highest	22
httpclient-4.3.1.jar	cpe:/a:apache:httpclient:4.3.1	org.apache.httpcomponents:httpclient:4.3.1	Medium	2	Highest	28
spring-core-4.1.4.RELEASE.jar	cpe:/a:pivotal:spring_framework:4.1.4 cpe:/a:pivotal_software:spring_framework:4.1.4	org.springframework:spring-core:4.1.4.RELEASE ✓	High	7	Highest	28
serialization.xstream.jar	cpe:/a:xstream_project:xstream:0.2.14	org.openmrs.module:serialization.xstream-omod:0.2.14	Medium	2	Low	15
htmlwidgets-api-1.9.0.jar	cpe:/a:widgets_project:widgets:1.9.0	org.openmrs.module:htmlwidgets-api:1.9.0	Medium	1	Low	22
spring-jms-3.0.5.RELEASE.jar	cpe:/a:vmware:springsource_spring_framework:3.0.5 cpe:/a:pivotal:spring_framework:3.0.5 cpe:/a:pivotal_software:spring_framework:3.0.5 cpe:/a:springsource:spring_framework:3.0.5	org.springframework:spring-jms:3.0.5.RELEASE ✓	High	14	Highest	26
appui-api-1.8.0.jar	cpe:/a:app_project:app:1.8.0	org.openmrs.module:appui-api:1.8.0	Medium	1	Low	21
jackson-databind-2.9.0.jar	cpe:/a:fasterxml:jackson-databind:2.9.0 cpe:/a:fasterxml:jackson:2.9.0	com.fasterxml.jackson.core:jackson-databind:2.9.0	High	3	Highest	35
activemq-protobuf-1.1.jar	cpe:/a:apache:activemq:1.1	org.apache.activemq.protobuf:activemq-protobuf:1.1	High	14	Highest	22
registrationapp.jar (shaded: org.openmrs.module:registrationapp-omod:1.12.0)	cpe:/a:app_project:app:1.12.0	org.openmrs.module:registrationapp-omod:1.12.0	Medium	1	Low	13
appui.jar (shaded: org.openmrs.module:appui-omod:1.8.0)	cpe:/a:app_project:app:1.8.0	org.openmrs.module:appui-omod:1.8.0	Medium	1	Low	13
htmlwidgets.jar (shaded: org.openmrs.module:htmlwidgets-omod:1.9.0)	cpe:/a:widgets_project:widgets:1.9.0	org.openmrs.module:htmlwidgets-omod:1.9.0	Medium	1	Low	13
uicommons.jar (shaded: org.openmrs.module:uicommons-scss:2.6.0)	cpe:/a:content_project:content:2.6.0	org.openmrs.module:uicommons-scss:2.6.0	Medium	1	Low	13
ehcache-2.10.0.jar (shaded: com.fasterxml.jackson.core:jackson-databind:2.3.3)	cpe:/a:fasterxml:jackson-databind:2.3.3 cpe:/a:fasterxml:jackson:2.3.3	com.fasterxml.jackson.core:jackson-databind:2.3.3	High	5	Highest	16
ehcache-2.10.0.jar (shaded: org.eclipse.jetty:jetty-continuation:8.1.15.v20140411)	cpe:/a:jetty:jetty:8.1.15.v20140411 cpe:/a:eclipse:jetty:8.1.15.v20140411	org.eclipse.jetty:jetty-continuation:8.1.15.v20140411	High	4	Low	15
ehcache-2.10.0.jar (shaded: org.eclipse.jetty:jetty-http:8.1.15.v20140411)	cpe:/a:jetty:jetty:8.1.15.v20140411 cpe:/a:eclipse:jetty:8.1.15.v20140411	org.eclipse.jetty:jetty-http:8.1.15.v20140411	High	4	Low	13
ehcache-2.10.0.jar (shaded: org.eclipse.jetty:jetty-security:8.1.15.v20140411)	cpe:/a:jetty:jetty:8.1.15.v20140411 cpe:/a:eclipse:jetty:8.1.15.v20140411	org.eclipse.jetty:jetty-security:8.1.15.v20140411	High	4	Low	15
ehcache-2.10.0.jar (shaded: org.eclipse.jetty:jetty-server:8.1.15.v20140411)	cpe:/a:jetty:jetty:8.1.15.v20140411 cpe:/a:eclipse:jetty:8.1.15.v20140411	org.eclipse.jetty:jetty-server:8.1.15.v20140411	High	4	Low	15
ehcache-2.10.0.jar (shaded: org.eclipse.jetty:jetty-servlet:8.1.15.v20140411)	cpe:/a:jetty:jetty:8.1.15.v20140411 cpe:/a:eclipse:jetty:8.1.15.v20140411	org.eclipse.jetty:jetty-servlet:8.1.15.v20140411	High	4	Low	15
ehcache-2.10.0.jar (shaded: org.eclipse.jetty:jetty-util:8.1.15.v20140411)	cpe:/a:jetty:jetty:8.1.15.v20140411 cpe:/a:eclipse:jetty:8.1.15.v20140411	org.eclipse.jetty:jetty-util:8.1.15.v20140411	High	4	Low	15

Dependency	CPE	Coordinates	Highest Severity	CVE Count	CPE Confidence	Evidence Count
formentryapp.jar (shaded: org.openmrs.module:formentryapp-omod:1.4.2)	cpe:/a:app_project:app:1.4.2	org.openmrs.module:formentryapp-omod:1.4.2	Medium	1	Low	13
appframework.jar (shaded: org.openmrs.module:appframework-omod:2.11.0)	cpe:/a:app_project:app:2.11.0	org.openmrs.module:appframework-omod:2.11.0	Medium	1	Low	13

Dependencies

chartsearch-server-2.1.0.jar

Description:

Solr server project for ChartSearch

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\chartsearch\lib\chartsearch-server-2.1.0.jar
MD5: c0d1f9bfef6c08764f550e2abd14200d
SHA1: 79e742c4ead92fcf67269277498dc0e6e6ef2810
SHA256:2038ed4329cfd6ae13a8b26b7e85c33a4e0451dd94c9a8700fb64e910c741348

Evidence

Related Dependencies

Identifiers

- **maven:** org.openmrs.module:chartsearch-server:2.1.0 *Confidence*:High
- **cpe:** cpe:/a:apache:solr:2.1.0 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2012-6612 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

The (1) UpdateRequestHandler for XSLT or (2) XPathEntityProcessor in Apache Solr before 4.1 allows remote attackers to have an unspecified impact via XML data containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, different vectors than CVE-2013-6407.

- CONFIRM - http://svn.apache.org/viewvc/lucene/dev/branches/branch_4x/solr/CHANGES.txt?view=markup
- CONFIRM - https://issues.apache.org/jira/browse/SOLR-3895
- REDHAT - RHSA-2013:1844
- REDHAT - RHSA-2014:0029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:solr:4.0.0:alpha and all previous versions
- ...

CVE-2013-6397 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Directory traversal vulnerability in SolrResourceLoader in Apache Solr before 4.6 allows remote attackers to read arbitrary files via a .. (dot dot) or full pathname in the tr parameter to solr/select/, when the response writer (wt parameter) is set to XSLT. NOTE: this can be leveraged using a separate XXE (XML eXternal Entity) vulnerability to allow access to files across restricted network boundaries.

- BID - 63935
- CONFIRM - http://lucene.apache.org/solr/4_6_0/changes/Changes.html
- CONFIRM - https://issues.apache.org/jira/browse/SOLR-4882
- MISC - http://www.agarri.fr/kom/archives/2013/11/27/compromising_an_unreachable_solr_server_with_cve-2013-6397/index.html
- MLIST - [oss-security] 20131126 Re: CVE request: Apache Solr 4.6.0
- REDHAT - RHSA-2013:1844
- REDHAT - RHSA-2014:0029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:solr:4.5.1 and all previous versions
- ...

CVE-2013-6407 suppress

Severity:Medium
CVSS Score: 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)

The UpdateRequestHandler for XML in Apache Solr before 4.1 allows remote attackers to have an unspecified impact via XML data containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.

- CONFIRM - http://svn.apache.org/viewvc/lucene/dev/branches/branch_4x/solr/CHANGES.txt?view=markup
- CONFIRM - https://issues.apache.org/jira/browse/SOLR-3895
- MLIST - [oss-security] 20131128 Re: CVE Request: Apache Solr XXE
- REDHAT - RHSA-2013:1844
- REDHAT - RHSA-2014:0029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:solr:4.0.0:alpha and all previous versions
- ...

CVE-2013-6408 suppress

Severity:Medium
CVSS Score: 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)

The DocumentAnalysisRequestHandler in Apache Solr before 4.3.1 does not properly use the EmptyEntityResolver, which allows remote attackers to have an unspecified impact via XML data containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-6407.

- CONFIRM - http://svn.apache.org/viewvc/lucene/dev/branches/branch_4x/solr/CHANGES.txt?view=markup
- CONFIRM - https://issues.apache.org/jira/browse/SOLR-4881
- MLIST - [oss-security] 20131128 Re: CVE Request: Apache Solr XXE
- REDHAT - RHSA-2013:1844
- REDHAT - RHSA-2014:0029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:solr:4.3.0 and all previous versions
- ...

CVE-2015-8795 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Multiple cross-site scripting (XSS) vulnerabilities in the Admin UI in Apache Solr before 5.1 allow remote attackers to inject arbitrary web script or HTML via crafted fields that are mishandled during the rendering of the (1) Analysis page, related to webapp/web/js/scripts/analysis.js or (2) Schema-Browser page, related to webapp/web/js/scripts/schema-browser.js.

- CONFIRM - https://issues.apache.org/jira/browse/SOLR-7346

Vulnerable Software & Versions:

- cpe:/a:apache:solr:5.0 and all previous versions

CVE-2015-8796 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in webapp/web/js/scripts/schema-browser.js in the Admin UI in Apache Solr before 5.3 allows remote attackers to inject arbitrary web script or HTML via a crafted schema-browse URL.

- BID - 85205
- CONFIRM - https://issues.apache.org/jira/browse/SOLR-7920

Vulnerable Software & Versions:

- cpe:/a:apache:solr:5.2.1 and all previous versions

CVE-2015-8797 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in webapp/web/js/scripts/plugins.js in the stats page in the Admin UI in Apache Solr before 5.3.1 allows remote attackers to inject arbitrary web script or HTML via the entry parameter to a plugins/cache URI.

- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21975544
- CONFIRM - https://issues.apache.org/jira/browse/SOLR-7949

Vulnerable Software & Versions:

- cpe:/a:apache:solr:5.3 and all previous versions

CVE-2017-3163 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

When using the Index Replication feature, Apache Solr nodes can pull index files from a master/leader node using an HTTP API which accepts a file name. However, Solr before 5.5.4 and 6.x before 6.4.1 did not validate the file name, hence it was possible to craft a special request involving path traversal, leaving any file readable to the Solr server process exposed. Solr servers protected and restricted by firewall rules and/or authentication would not be at risk since only trusted clients and users would gain direct HTTP access.

- DEBIAN - DSA-4124
- MLIST - [solr-user] 20170215 [SECURITY] CVE-2017-3163 Apache Solr ReplicationHandler path traversal attack
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:solr:5.5.3 and all previous versions
- ...

hibernate-validator-4.2.0.Final.jar

Description:

Hibernate's Bean Validation (JSR-303) reference implementation.

License:

http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\tomcat\webapps\openmrs-standalone\WEB-INF\lib\hibernate-validator-4.2.0.Final.jar
MD5: 2b6b64bce7156ca6e9b7f5e6a0a6de7c
SHA1: eac2db0a9d86a9749724fe93d43afffa8106f25e
SHA256:38dd0af5fdad46bb30270f2d987136ad5ea9bc16927182af7d639e78828133a5

Evidence

Related Dependencies

Identifiers

- **maven:** org.hibernate:hibernate-validator:4.2.0.Final ✓ *Confidence*:Highest
- **cpe:** cpe:/a:hibernate:hibernate_validator:4.2.0 *Confidence*:Highest suppress

Published Vulnerabilities

CVE-2014-3558 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-264 Permissions, Privileges, and Access Controls

ReflectionHelper (org.hibernate.validator.util.ReflectionHelper) in Hibernate Validator 4.1.0 before 4.2.1, 4.3.x before 4.3.2, and 5.x before 5.1.2 allows attackers to bypass Java Security Manager (JSM) restrictions and execute restricted reflection calls via a crafted application.

- CONFIRM - https://hibernate.atlassian.net/browse/HV-912
- MISC - https://github.com/victims/victims-cve-db/blob/master/database/java/2014/3558.yaml
- REDHAT - RHSA-2014:1285
- REDHAT - RHSA-2014:1286
- REDHAT - RHSA-2014:1287
- REDHAT - RHSA-2014:1288
- REDHAT - RHSA-2015:0125
- REDHAT - RHSA-2015:0720

Vulnerable Software & Versions: (show all)

- cpe:/a:hibernate:hibernate_validator:4.2.0
- ...

jackson-databind-2.5.4.jar

Description:

General data-binding functionality for Jackson: works on core streaming API

License:

http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\fhir\lib\jackson-databind-2.5.4.jar
MD5: a6c0a282905c8f5c4a80a36c75526485
SHA1: 5dfa42af84584b4a862ea488da84bbbebbb06c35
SHA256:338b9aa87b8b17d33026defdbd8d9c1ec498bf355e8b949381f303ea23c261ac

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:fasterxml:jackson-databind:2.5.4 *Confidence*:Highest suppress
- **maven:** com.fasterxml.jackson.core:jackson-databind:2.5.4 *Confidence*:High
- **cpe:** cpe:/a:fasterxml:jackson:2.5.4 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2017-15095 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-502 Deserialization of Untrusted Data

A deserialization flaw was discovered in the jackson-databind in versions before 2.8.10 and 2.9.1, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper. This issue extends the previous flaw CVE-2017-7525 by blacklisting more classes that could be used maliciously.

- BID - 103880
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1680
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1737
- CONFIRM - https://security.netapp.com/advisory/ntap-20171214-0003/
- DEBIAN - DSA-4037
- REDHAT - RHSA-2017:3189
- REDHAT - RHSA-2017:3190
- REDHAT - RHSA-2018:0342
- REDHAT - RHSA-2018:0478
- REDHAT - RHSA-2018:0479
- REDHAT - RHSA-2018:0480
- REDHAT - RHSA-2018:0481
- REDHAT - RHSA-2018:0576
- REDHAT - RHSA-2018:0577
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451
- SECTRACK - 1039769

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.5.4
- ...

CVE-2017-17485 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-94 Improper Control of Generation of Code ('Code Injection')

FasterXML jackson-databind through 2.8.10 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the Spring libraries are available in the classpath.

- BUGTRAQ - 20180109 CVE-2017-17485: one more way of rce in jackson-databind when defaultTyping+objects are used
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1855
- CONFIRM - https://security.netapp.com/advisory/ntap-20180201-0003/
- DEBIAN - DSA-4114
- MISC - https://github.com/irsl/jackson-rce-via-spel/
- REDHAT - RHSA-2018:0116
- REDHAT - RHSA-2018:0342
- REDHAT - RHSA-2018:0478
- REDHAT - RHSA-2018:0479
- REDHAT - RHSA-2018:0480
- REDHAT - RHSA-2018:0481
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.8.10 and all previous versions
- ...

CVE-2017-7525 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-502 Deserialization of Untrusted Data

A deserialization flaw was discovered in the jackson-databind, versions before 2.6.7.1, 2.7.9.1 and 2.8.9, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper.

- BID - 99623
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1462702
- CONFIRM - https://cwiki.apache.org/confluence/display/WW/S2-055

- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1599
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1723
- CONFIRM - https://security.netapp.com/advisory/ntap-20171214-0002/
- DEBIAN - DSA-4004
- REDHAT - RHSA-2017:1834
- REDHAT - RHSA-2017:1835
- REDHAT - RHSA-2017:1836
- REDHAT - RHSA-2017:1837
- REDHAT - RHSA-2017:1839
- REDHAT - RHSA-2017:1840
- REDHAT - RHSA-2017:2477
- REDHAT - RHSA-2017:2546
- REDHAT - RHSA-2017:2547
- REDHAT - RHSA-2017:2633
- REDHAT - RHSA-2017:2635
- REDHAT - RHSA-2017:2636
- REDHAT - RHSA-2017:2637
- REDHAT - RHSA-2017:2638
- REDHAT - RHSA-2017:3141
- REDHAT - RHSA-2017:3454
- REDHAT - RHSA-2017:3455
- REDHAT - RHSA-2017:3456
- REDHAT - RHSA-2017:3458
- REDHAT - RHSA-2018:0294
- REDHAT - RHSA-2018:0342
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- SECTRACK - 1039744
- SECTRACK - 1039947
- SECTRACK - 1040360

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.5.4
- ...

CVE-2018-5968 suppress

Severity:Medium
CVSS Score: 5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
CWE: CWE-184 Incomplete Blacklist

FasterXML jackson-databind through 2.8.11 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 and CVE-2017-17485 deserialization flaws. This is exploitable via two different gadgets that bypass a blacklist.

- CONFIRM - https://security.netapp.com/advisory/ntap-20180423-0002/
- DEBIAN - DSA-4114
- MISC - https://github.com/FasterXML/jackson-databind/issues/1899
- REDHAT - RHSA-2018:0478
- REDHAT - RHSA-2018:0479
- REDHAT - RHSA-2018:0480
- REDHAT - RHSA-2018:0481
- REDHAT - RHSA-2018:1525

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.8.11 and all previous versions
- ...

CVE-2018-7489 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-184 Incomplete Blacklist

FasterXML jackson-databind before 2.8.11.1 and 2.9.x before 2.9.5 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the c3p0 libraries are available in the classpath.

- BID - 103203
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1931
- CONFIRM - https://security.netapp.com/advisory/ntap-20180328-0001/
- DEBIAN - DSA-4190
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451
- REDHAT - RHSA-2018:1786
- REDHAT - RHSA-2018:2088
- REDHAT - RHSA-2018:2089
- REDHAT - RHSA-2018:2090
- SECTRACK - 1040693

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.5.4
- ...

jetty-jmx-8.1.10.v20130312.jar

Description:

JMX management artifact for jetty.

License:

http://www.apache.org/licenses/LICENSE-2.0, http://www.eclipse.org/org/documents/epl-v10.php

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\chartsearch\lib\jetty-jmx-8.1.10.v20130312.jar
MD5: f8db4d656961a767283aa456209a445b
SHA1: 6e48870e2af2caf2a77751eae3a79bfcf6b90a78
SHA256:d55d234ce25a0ecac76beb0704c91216839220c66fe0eadfbfa10363ebab39fe

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:eclipse:jetty:8.1.10.v20130312 *Confidence*:Low suppress
- **cpe:** cpe:/a:jetty:jetty:8.1.10.v20130312 *Confidence*:Low suppress
- **maven:** org.eclipse.jetty:jetty-jmx:8.1.10.v20130312 *Confidence*:High

Published Vulnerabilities

CVE-2017-7656 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-284 Improper Access Control

In Eclipse Jetty, versions 9.2.x and older, 9.3.x (all configurations), and 9.4.x (non-default configuration with RFC2616 compliance enabled), HTTP/0.9 is handled poorly. An HTTP/1 style request line (i.e. method space URI space version) that declares a version of HTTP/0.9 was accepted and treated as a 0.9 request. If deployed behind an intermediary that also accepted and passed through the 0.9 version (but did not act on it), then the response sent could be interpreted by the intermediary as HTTP/1 headers. This could be used to poison the cache if the server allowed the origin client to generate arbitrary content in the response.

- CONFIRM - https://bugs.eclipse.org/bugs/show_bug.cgi?id=535667
- DEBIAN - DSA-4278
- SECTRACK - 1041194

Vulnerable Software & Versions: (show all)

- cpe:/a:eclipse:jetty:9.2.26 and all previous versions
- ...

CVE-2017-7657 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-190 Integer Overflow or Wraparound

In Eclipse Jetty, versions 9.2.x and older, 9.3.x (all configurations), and 9.4.x (non-default configuration with RFC2616 compliance enabled), transfer-encoding chunks are handled poorly. The chunk length parsing was vulnerable to an integer overflow. Thus a large chunk size could be interpreted as a smaller chunk size and content sent as chunk body could be interpreted as a pipelined request. If Jetty was deployed behind an intermediary that imposed some authorization and that intermediary allowed arbitrarily large chunks to be passed on unchanged, then this flaw could be used to bypass the authorization imposed by the intermediary as the fake pipelined request would not be interpreted by the intermediary as a request.

- CONFIRM - https://bugs.eclipse.org/bugs/show_bug.cgi?id=535668
- DEBIAN - DSA-4278
- SECTRACK - 1041194

Vulnerable Software & Versions: (show all)

- cpe:/a:eclipse:jetty:9.2.26 and all previous versions
- ...

CVE-2017-7658 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-19 Data Processing Errors

In Eclipse Jetty Server, versions 9.2.x and older, 9.3.x (all non HTTP/1.x configurations), and 9.4.x (all HTTP/1.x configurations), when presented with two content-lengths headers, Jetty ignored the second. When presented with a content-length and a chunked encoding header, the content-length was ignored (as per RFC 2616). If an intermediary decided on the shorter length, but still passed on the longer body, then body content could be interpreted by Jetty as a pipelined request. If the intermediary was imposing authorization, the fake pipelined request would bypass that authorization.

- CONFIRM - https://bugs.eclipse.org/bugs/show_bug.cgi?id=535669
- DEBIAN - DSA-4278
- SECTRACK - 1041194

Vulnerable Software & Versions: (show all)

- cpe:/a:eclipse:jetty:9.2.26 and all previous versions
- ...

CVE-2017-9735 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-200 Information Exposure

Jetty through 9.4.x is prone to a timing channel in util/security/Password.java, which makes it easier for remote attackers to obtain access by observing elapsed times before rejection of incorrect passwords.

- BID - 99104
- MISC - https://bugs.debian.org/864631
- MISC - https://github.com/eclipse/jetty.project/issues/1556

Vulnerable Software & Versions:

- cpe:/a:eclipse:jetty:9.4.6:20170531 and all previous versions

xalan-2.7.0.jar

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\tomcat\webapps\openmrs-standalone\WEB-INF\lib\xalan-2.7.0.jar
MD5: a018d032c21a873225e702b36b171a10
SHA1: a33c0097f1c70b20fa7ded220ea317eb3500515e
SHA256:bf1f065efd6e3d5cb964db4130815752015873338999d23dcafc2dbc89fc7d9b

Evidence

Related Dependencies

Identifiers

- **maven:** xalan:xalan:2.7.0 ✓ *Confidence*:Highest
- **cpe:** cpe:/a:apache:xalan-java:2.7.0 *Confidence*:Highest suppress

Published Vulnerabilities

CVE-2014-0107 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

The TransformerFactory in Apache Xalan-Java before 2.7.2 does not properly restrict access to certain properties when FEATURE_SECURE_PROCESSING is enabled, which allows remote attackers to bypass expected restrictions and load arbitrary classes or access external resources via a crafted (1) xalan:content-header, (2) xalan:entities, (3) xslt:content-header, or (4) xslt:entities property, or a Java property that is bound to the XSLT 1.0 system-property function.

- BID - 66397
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1581058
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21674334
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676093
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21677145
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21680703
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21681933
- CONFIRM - http://www.ibm.com/support/docview.wss?uid=swg21677967
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05324755
- CONFIRM - https://issues.apache.org/jira/browse/XALANJ-2435
- DEBIAN - DSA-2886
- GENTOO - GLSA-201604-02
- MISC - http://www.ocert.org/advisories/ocert-2014-002.html
- REDHAT - RHSA-2014:0348
- REDHAT - RHSA-2014:1351
- REDHAT - RHSA-2015:1888
- SECTRACK - 1034711
- SECTRACK - 1034716
- SECUNIA - 59151
- SECUNIA - 59247
- SECUNIA - 59290
- SECUNIA - 59291
- SECUNIA - 59515
- XF - apache-xalanjava-cve20140107-sec-bypass(92023)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:xalan-java:2.7.0
- ...

org.restlet-2.1.1.jar

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\chartsearch\lib\org.restlet-2.1.1.jar
MD5: 9bdf03f129c6ec8d0da680a979013e55
SHA1: e12c23b962c925f2681729afa1e40066a350ad27
SHA256:999570677d7165d9c9ed5fc34b3af20f50e01eeacf50813a821e565a2fb6838d

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:restlet:restlet_framework:2.1.1 *Confidence*:Highest suppress
- **cpe:** cpe:/a:restlet:restlet:2.1.1 *Confidence*:Highest suppress

Published Vulnerabilities

CVE-2013-4221 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-16 Configuration

The default configuration of the ObjectRepresentation class in Restlet before 2.1.4 deserializes objects from untrusted sources using the Java XMLDecoder, which allows remote attackers to execute arbitrary Java code via crafted XML.

- CONFIRM - http://restlet.org/learn/2.1/changes
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=995275
- CONFIRM - https://github.com/restlet/restlet-framework-java/issues/774
- MISC - http://blog.diniscruz.com/2013/08/using-xmldecoder-to-execute-server-side.html
- REDHAT - RHSA-2013:1410
- REDHAT - RHSA-2013:1862

Vulnerable Software & Versions: (show all)

- cpe:/a:restlet:restlet:2.1.1
- ...

CVE-2013-4271 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-502 Deserialization of Untrusted Data

The default configuration of the ObjectRepresentation class in Restlet before 2.1.4 deserializes objects from untrusted sources, which allows remote attackers to execute arbitrary Java code via a serialized object, a different vulnerability than CVE-2013-4221.

- CONFIRM - http://restlet.org/learn/2.1/changes
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=999735
- CONFIRM - https://github.com/restlet/restlet-framework-java/issues/778
- REDHAT - RHSA-2013:1410
- REDHAT - RHSA-2013:1862

Vulnerable Software & Versions: (show all)

- cpe:/a:restlet:restlet:2.1.1
- ...

CVE-2014-1868 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

Restlet Framework 2.1.x before 2.1.7 and 2.x.x before 2.2 RC1, when using XMLRepresentation or XML serializers, allows attackers to cause a denial of service via an XML Entity Expansion (XEE) attack.

- CONFIRM - https://github.com/restlet/restlet-framework-java/wiki/XEE-security-enhancements
- XF - restlet-framework-cve20141868-dos(91181)

Vulnerable Software & Versions: (show all)

- cpe:/a:restlet:restlet_framework:2.1.1
- ...

CVE-2017-14868 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-611 Improper Restriction of XML External Entity Reference ('XXE')

Restlet Framework before 2.3.11, when using SimpleXMLProvider, allows remote attackers to access arbitrary files via an XXE attack in a REST API HTTP request. This affects use of the Jax-rs extension.

- MISC - https://github.com/restlet/restlet-framework-java/issues/1286
- MISC - https://github.com/restlet/restlet-framework-java/wiki/XEE-security-enhancements

- MISC - https://lgtm.com/blog/restlet_CVE-2017-14868

Vulnerable Software & Versions: (show all)

- cpe:/a:restlet:restlet:2.1.1
- ...

CVE-2017-14949 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-611 Improper Restriction of XML External Entity Reference ('XXE')

Restlet Framework before 2.3.12 allows remote attackers to access arbitrary files via a crafted REST API HTTP request that conducts an XXE attack, because only general external entities (not parameter external entities) are properly considered. This is related to XmlRepresentation, DOMRepresentation, SaxRepresentation, and JacksonRepresentation.

- MISC - https://github.com/restlet/restlet-framework-java/wiki/XEE-security-enhancements
- MISC - https://lgtm.com/blog/restlet_CVE-2017-14949

Vulnerable Software & Versions: (show all)

- cpe:/a:restlet:restlet:2.1.1
- ...

poi-3.12.jar

Description:

Apache POI - Java API To Access Microsoft Format Files

License:

The Apache Software License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\reporting\lib\poi-3.12.jar
MD5: c22098095e289dd8546d1565bc1a4c7d
SHA1: 8be19a6a1fa08e934a497929f360111a4d2e5115
SHA256:aef9a5c3895c7fa05d8f72f477d817d3c2a11c8f4760c3d0951b86a7eb07f151

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:apache:poi:3.12 *Confidence*:Low suppress
- **maven:** org.apache.poi:poi:3.12 ✓ *Confidence*:Highest

Published Vulnerabilities

CVE-2016-5000 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-611 Improper Restriction of XML External Entity Reference ('XXE')

The XLSX2CSV example in Apache POI before 3.14 allows remote attackers to read arbitrary files via a crafted OpenXML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.

- BID - 92100
- BUGTRAQ - 20160722 [CVE-2016-5000] XML External Entity (XXE) Vulnerability in Apache POI's XLSX2CSV Example
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21996759
- MLIST - [users] 20160722 [CVE-2016-5000] XML External Entity (XXE) Vulnerability in Apache POI's XLSX2CSV Example
- SECTRACK - 1037741

Vulnerable Software & Versions:

- cpe:/a:apache:poi:3.13 and all previous versions

CVE-2017-5644 suppress

Severity:High
CVSS Score: 7.1 (AV:N/AC:M/Au:N/C:N/I:N/A:C)
CWE: CWE-399 Resource Management Errors

Apache POI in versions prior to release 3.15 allows remote attackers to cause a denial of service (CPU consumption) via a specially crafted OOXML file, aka an XML Entity Expansion (XEE) attack.

- BID - 96983
- CONFIRM - http://poi.apache.org/#20+March+2017+-+CVE-2017-5644+-+Possible+DOS+%28Denial+of+Service%29+in+Apache+POI+versions+prior+to+3.15

Vulnerable Software & Versions:

- cpe:/a:apache:poi:3.14 and all previous versions

xercesImpl-2.8.0.jar

Description:

Xerces2 is the next generation of high performance, fully compliant XML parsers in the Apache Xerces family. This new version of Xerces introduces the Xerces Native Interface (XNI), a complete framework for building parser components and configurations that is extremely modular and easy to program.

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\tomcat\webapps\openmrs-standalone\WEB-INF\lib\xercesImpl-2.8.0.jar
MD5: 7eb2db331a62e74744ab79aab5b454bd
SHA1: cfd3ebe2f8034e660344f9108c3e2daf78c29cc3
SHA256:13bb155eb24f03229798b3fb409d3a2c47e332d79c34d4b4b1ad39b0a917f3b8

Evidence

Related Dependencies

Identifiers

- **maven:** xerces:xercesImpl:2.8.0 ✓ *Confidence*:Highest
- **cpe:** cpe:/a:apache:xerces2_java:2.8.0 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2012-0881 suppress

Severity:High
CVSS Score: 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
CWE: CWE-399 Resource Management Errors

Apache Xerces2 Java allows remote attackers to cause a denial of service (CPU consumption) via a crafted message to an XML service, which triggers hash table collisions.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=787104
- MLIST - [oss-security] 20140708 Summer bug cleaning - some Hash DoS stuff

Vulnerable Software & Versions:

- cpe:/a:apache:xerces2_java:2.11.0 and all previous versions

registrationapp-api-1.12.0.jar

Description:

API project for RegistrationApp

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\registrationapp\lib\registrationapp-api-1.12.0.jar
MD5: 3ed6639bb949a1f6aab2bb0fbf622ed0
SHA1: e54dbbb41c939da2179432929ebea0879461432a
SHA256:f9b343b2dab9bf9ea10e0eb16c2b5b9d12781ec3d24928376b1e539a7b0e9df2

Evidence

Related Dependencies

Identifiers

- **maven:** org.openmrs.module:registrationapp-api:1.12.0 *Confidence*:High
- **cpe:** cpe:/a:app_project:app:1.12.0 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2018-13661 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-190 Integer Overflow or Wraparound

The mintToken function of a smart contract implementation for APP, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value.

- MISC - https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md
- MISC - https://github.com/BlockChainsSecurity/EtherTokens/tree/master/APP

Vulnerable Software & Versions:

- cpe:/a:app_project:app:-

stax-api-1.0.1.jar

Description:

StAX API is the standard java XML processing API defined by JSR-173

License:

The Apache Software License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\reportingcompatibility\lib\stax-api-1.0.1.jar
MD5: 7d436a53c64490bee564c576babb36b4
SHA1: 49c100caf72d658aca8e58bd74a4ba90fa2b0d70
SHA256:d1968436fc216c901fb9b82c7e878b50fd1d30091676da95b2edd3a9c0ccf92e

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:st_project:st:1.0.1 *Confidence*:Low suppress
- **maven:** stax:stax-api:1.0.1 ✓ *Confidence*:Highest

Published Vulnerabilities

CVE-2017-16224 suppress

Severity:Medium
CVSS Score: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)
CWE: CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

st is a module for serving static files. An attacker is able to craft a request that results in an HTTP 301 (redirect) to an entirely different domain. A request for: http://some.server.com//nodesecurity.org/%2e%2e would result in a 301 to //nodesecurity.org/%2e%2e which most browsers treat as a proper redirect as // is translated into the current schema being used. Mitigating factor: In order for this to work, st must be serving from the root of a server (/) rather than the typical sub directory (/static/) and the redirect URL will end with some form of URL encoded .. ("%2e%2e", "%2e.", ".%2e").

- MISC - https://nodesecurity.io/advisories/547

Vulnerable Software & Versions:

- cpe:/a:st_project:st:1.2.1::~~~node.js~~ and all previous versions

jackson-databind-2.8.1.jar

Description:

General data-binding functionality for Jackson: works on core streaming API

License:

http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\metadatamapping\lib\jackson-databind-2.8.1.jar
MD5: ea9e974ead306a615eb8d8cb50fb93d9

SHA1: c04eb2cc599cd1742889bfa7cc41878db0d152f5
SHA256:0bbf7a039135fefee20d6205bef4f72a42eed5713a144acfb32d422ec450cc9d

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:fasterxml:jackson-databind:2.8.1 *Confidence*:Highest suppress
- **maven:** com.fasterxml.jackson.core:jackson-databind:2.8.1 *Confidence*:High
- **cpe:** cpe:/a:fasterxml:jackson:2.8.1 *Confidence*:Highest suppress

Published Vulnerabilities

CVE-2017-15095 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-502 Deserialization of Untrusted Data

A deserialization flaw was discovered in the jackson-databind in versions before 2.8.10 and 2.9.1, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper. This issue extends the previous flaw CVE-2017-7525 by blacklisting more classes that could be used maliciously.

- BID - 103880
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1680
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1737
- CONFIRM - https://security.netapp.com/advisory/ntap-20171214-0003/
- DEBIAN - DSA-4037
- REDHAT - RHSA-2017:3189
- REDHAT - RHSA-2017:3190
- REDHAT - RHSA-2018:0342
- REDHAT - RHSA-2018:0478
- REDHAT - RHSA-2018:0479
- REDHAT - RHSA-2018:0480
- REDHAT - RHSA-2018:0481
- REDHAT - RHSA-2018:0576
- REDHAT - RHSA-2018:0577
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451
- SECTRACK - 1039769

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.8.1
- ...

CVE-2017-17485 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-94 Improper Control of Generation of Code ('Code Injection')

FasterXML jackson-databind through 2.8.10 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the Spring libraries are available in the classpath.

- BUGTRAQ - 20180109 CVE-2017-17485: one more way of rce in jackson-databind when defaultTyping+objects are used
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1855
- CONFIRM - https://security.netapp.com/advisory/ntap-20180201-0003/
- DEBIAN - DSA-4114
- MISC - https://github.com/irsl/jackson-rce-via-spel/
- REDHAT - RHSA-2018:0116
- REDHAT - RHSA-2018:0342
- REDHAT - RHSA-2018:0478
- REDHAT - RHSA-2018:0479
- REDHAT - RHSA-2018:0480
- REDHAT - RHSA-2018:0481
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.8.10 and all previous versions
- ...

CVE-2017-7525 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-502 Deserialization of Untrusted Data

A deserialization flaw was discovered in the jackson-databind, versions before 2.6.7.1, 2.7.9.1 and 2.8.9, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper.

- BID - 99623
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1462702
- CONFIRM - https://cwiki.apache.org/confluence/display/WW/S2-055
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1599
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1723
- CONFIRM - https://security.netapp.com/advisory/ntap-20171214-0002/
- DEBIAN - DSA-4004
- REDHAT - RHSA-2017:1834
- REDHAT - RHSA-2017:1835
- REDHAT - RHSA-2017:1836
- REDHAT - RHSA-2017:1837
- REDHAT - RHSA-2017:1839
- REDHAT - RHSA-2017:1840
- REDHAT - RHSA-2017:2477
- REDHAT - RHSA-2017:2546
- REDHAT - RHSA-2017:2547
- REDHAT - RHSA-2017:2633
- REDHAT - RHSA-2017:2635
- REDHAT - RHSA-2017:2636
- REDHAT - RHSA-2017:2637
- REDHAT - RHSA-2017:2638
- REDHAT - RHSA-2017:3141
- REDHAT - RHSA-2017:3454
- REDHAT - RHSA-2017:3455
- REDHAT - RHSA-2017:3456
- REDHAT - RHSA-2017:3458
- REDHAT - RHSA-2018:0294
- REDHAT - RHSA-2018:0342
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- SECTRACK - 1039744
- SECTRACK - 1039947
- SECTRACK - 1040360

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.8.1
- ...

CVE-2018-5968 suppress

Severity:Medium
CVSS Score: 5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
CWE: CWE-184 Incomplete Blacklist

FasterXML jackson-databind through 2.8.11 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 and CVE-2017-17485 deserialization flaws. This is exploitable via two different gadgets that bypass a blacklist.

- CONFIRM - https://security.netapp.com/advisory/ntap-20180423-0002/
- DEBIAN - DSA-4114
- MISC - https://github.com/FasterXML/jackson-databind/issues/1899
- REDHAT - RHSA-2018:0478
- REDHAT - RHSA-2018:0479
- REDHAT - RHSA-2018:0480
- REDHAT - RHSA-2018:0481
- REDHAT - RHSA-2018:1525

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.8.11 and all previous versions
- ...

CVE-2018-7489 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-184 Incomplete Blacklist

FasterXML jackson-databind before 2.8.11.1 and 2.9.x before 2.9.5 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the c3p0 libraries are available in the classpath.

- BID - 103203
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1931
- CONFIRM - https://security.netapp.com/advisory/ntap-20180328-0001/
- DEBIAN - DSA-4190
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451
- REDHAT - RHSA-2018:1786
- REDHAT - RHSA-2018:2088
- REDHAT - RHSA-2018:2089
- REDHAT - RHSA-2018:2090
- SECTRACK - 1040693

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.8.1
- ...

activemq-core-5.4.3.jar

Description:

The ActiveMQ Message Broker and Client implementations

License:

http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\event\lib\activemq-core-5.4.3.jar
MD5: 07f02054255d8c8fd769bfa5ba33f286
SHA1: 024d650bd3f379cc3dd3dc059438578ed93b2197
SHA256:9f045d70a68d591121a4ef9f767b762eb300d18ee1646bee4a4d5b9183e6b0f7

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:apache:activemq:5.4.3 *Confidence*:Highest suppress
- **maven:** org.apache.activemq:activemq-core:5.4.3 *Confidence*:High

Published Vulnerabilities

CVE-2011-4905 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-399 Resource Management Errors

Apache ActiveMQ before 5.6.0 allows remote attackers to cause a denial of service (file-descriptor exhaustion and broker crash or hang) by sending many openwire failover:tcp:// connection requests.

- BID - 50904
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1209700
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1211844
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-3294
- MLIST - [oss-security] 20111224 CVE Request for Apache ActiveMQ DoS
- MLIST - [oss-security] 20111225 Re: CVE Request for Apache ActiveMQ DoS

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2012-5784 suppress

Severity:Medium
CVSS Score: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)
CWE: CWE-20 Improper Input Validation

Apache Axis 1.4 and earlier, as used in PayPal Payments Pro, PayPal Mass Pay, PayPal Transactional Information SOAP, the Java Message Service implementation in Apache ActiveMQ, and other products, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- BID - 56408
- MISC - http://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf
- REDHAT - RHSA-2013:0269
- REDHAT - RHSA-2013:0683
- REDHAT - RHSA-2014:0037
- XF - apache-axis-ssl-spoofing(79829)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2012-6092 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Multiple cross-site scripting (XSS) vulnerabilities in the web demos in Apache ActiveMQ before 5.8.0 allow remote attackers to inject arbitrary web script or HTML via (1) the refresh parameter to PortfolioPublishServlet.java (aka demo/portfolioPublish or Market Data Publisher), or vectors involving (2) debug logs or (3) subscribe

messages in webapp/websocket/chat.js. NOTE: AMQ-4124 is covered by CVE-2012-6551.

- BID - 59400
- CONFIRM - http://activemq.apache.org/activemq-580-release.html
- CONFIRM - https://fisheye6.atlassian.com/changelog/activemq?cs=1399577
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4115
- CONFIRM - https://issues.apache.org/jira/secure/ReleaseNote.jspa?projectId=12311210&version=12323282
- REDHAT - RHSA-2013:1029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2012-6551 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-399 Resource Management Errors

The default configuration of Apache ActiveMQ before 5.8.0 enables a sample web application, which allows remote attackers to cause a denial of service (broker resource consumption) via HTTP requests.

- BID - 59401
- CONFIRM - http://activemq.apache.org/activemq-580-release.html
- CONFIRM - https://fisheye6.atlassian.com/changelog/activemq?cs=1404998
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4124
- CONFIRM - https://issues.apache.org/jira/secure/ReleaseNote.jspa?projectId=12311210&version=12323282
- MLIST - [dev] 20121022 [DISCUSS] - ActiveMQ out of the box - Should not include the demos
- REDHAT - RHSA-2013:1029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2013-1879 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in scheduled.jsp in Apache ActiveMQ 5.8.0 and earlier allows remote attackers to inject arbitrary web script or HTML via vectors involving the "cron of a message."

- BID - 61142
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4397
- REDHAT - RHSA-2013:1029
- XF - activemq-cve20131879-xss(85586)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.8.0 and all previous versions
- ...

CVE-2013-1880 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in the Portfolio publisher servlet in the demo web application in Apache ActiveMQ before 5.9.0 allows remote attackers to inject arbitrary web script or HTML via the refresh parameter to demo/portfolioPublish, a different vulnerability than CVE-2012-6092.

- BID - 65615
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=924447
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4398
- REDHAT - RHSA-2013:1029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.8.0 and all previous versions
- ...

CVE-2013-3060 suppress

Severity:Medium
CVSS Score: 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)
CWE: CWE-287 Improper Authentication

The web console in Apache ActiveMQ before 5.8.0 does not require authentication, which allows remote attackers to obtain sensitive information or cause a denial of service via HTTP requests.

- BID - 59402
- CONFIRM - http://activemq.apache.org/activemq-580-release.html
- CONFIRM - https://fisheye6.atlassian.com/changelog/activemq?cs=1404998
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4124
- CONFIRM - https://issues.apache.org/jira/secure/ReleaseNote.jspa?projectId=12311210&version=12323282
- MLIST - [dev] 20121022 [DISCUSS] - ActiveMQ out of the box - Should not include the demos
- REDHAT - RHSA-2013:1029
- REDHAT - RHSA-2013:1221

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2014-3576 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

The processControlCommand function in broker/TransportConnection.java in Apache ActiveMQ before 5.11.0 allows remote attackers to cause a denial of service (shutdown) via a shutdown command.

- BID - 76272
- BUGTRAQ - 20151106 [ANNOUNCE] CVE-2014-3576 - Apache ActiveMQ vulnerabilities
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
- CONFIRM - https://github.com/apache/activemq/commit/00921f2
- DEBIAN - DSA-3330
- MISC - http://packetstormsecurity.com/files/134274/Apache-ActiveMQ-5.10.1-Denial-Of-Service.html
- MLIST - [dev] 20150721 About CVE-2014-3576
- SECTRACK - 1033898

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.10.0 and all previous versions
- ...

CVE-2014-3600 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-611 Improper Restriction of XML External Entity Reference ('XXE')

XML external entity (XXE) vulnerability in Apache ActiveMQ 5.x before 5.10.1 allows remote consumers to have unspecified impact via vectors involving an XPath based selector when dequeuing XML messages.

- BID - 72510
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2014-3600-announcement.txt
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-5333
- MLIST - [oss-security] 20150205 [ANNOUNCE] CVE-2014-3600, CVE-2014-3612 and CVE-2014-8110 - Apache ActiveMQ vulnerabilities
- XF - apache-activemq-cve20143600-info-disc(100722)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2014-3612 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-287 Improper Authentication

The LDAPLoginModule implementation in the Java Authentication and Authorization Service (JAAS) in Apache ActiveMQ 5.x before 5.10.1 allows remote attackers to bypass authentication by logging in with an empty password and valid username, which triggers an unauthenticated bind. NOTE: this identifier has been SPLIT per ADT2 due to different vulnerability types. See CVE-2015-6524 for the use of wildcard operators in usernames.

- BID - 72513
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2014-3612-announcement.txt
- MLIST - [oss-security] 20150205 [ANNOUNCE] CVE-2014-3600, CVE-2014-3612 and CVE-2014-8110 - Apache ActiveMQ vulnerabilities
- REDHAT - RHSA-2015:0137
- REDHAT - RHSA-2015:0138

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2014-8110 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Multiple cross-site scripting (XSS) vulnerabilities in the web based administration console in Apache ActiveMQ 5.x before 5.10.1 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- BID - 72511
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2014-8110-announcement.txt
- MLIST - [oss-security] 20150205 [ANNOUNCE] CVE-2014-3600, CVE-2014-3612 and CVE-2014-8110 - Apache ActiveMQ vulnerabilities
- XF - apache-activemq-cve20148110-xss(100724)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2015-1830 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Directory traversal vulnerability in the fileserver upload/download functionality for blob messages in Apache ActiveMQ 5.x before 5.11.2 for Windows allows remote attackers to create JSP files in arbitrary directories via unspecified vectors.

- BID - 76452
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2015-1830-announcement.txt
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-15-407
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-15-407/
- SECTRACK - 1033315

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2015-5182 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-352 Cross-Site Request Forgery (CSRF)

Cross-site request forgery (CSRF) vulnerability in the jolokia API in A-MQ.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1248809

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:-

CVE-2015-5183 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-254 7PK - Security Features

The Hawtio console in A-MQ does not set HTTPOnly or Secure attributes on cookies.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1249182

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:-

CVE-2015-5184 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-254 7PK - Security Features

The Hawtio console in A-MQ allows remote attackers to obtain sensitive information and perform other unspecified impact.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1249183

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:-

CVE-2015-5254 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-20 Improper Input Validation

Apache ActiveMQ 5.x before 5.13.0 does not restrict the classes that can be serialized in the broker, which allows remote attackers to execute arbitrary code via a crafted serialized Java Message Service (JMS) ObjectMessage object.

- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2015-5254-announcement.txt
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05385680
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-6013
- DEBIAN - DSA-3524
- FEDORA - FEDORA-2015-7ca4368b0c
- FEDORA - FEDORA-2015-eefc5a6762
- MLIST - [oss-security] 20151208 [ANNOUNCE] CVE-2015-5254 - Unsafe deserialization in ActiveMQ
- REDHAT - RHSA-2016:0489
- REDHAT - RHSA-2016:2035
- REDHAT - RHSA-2016:2036

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2015-6524 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-255 Credentials Management

The LDAPLoginModule implementation in the Java Authentication and Authorization Service (JAAS) in Apache ActiveMQ 5.x before 5.10.1 allows wildcard operators in usernames, which allows remote attackers to obtain credentials via a brute force attack. NOTE: this identifier was SPLIT from CVE-2014-3612 per ADT2 due to different vulnerability types.

- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2014-3612-announcement.txt
- FEDORA - FEDORA-2015-5622085024
- FEDORA - FEDORA-2015-701a1e1a5f

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2016-0734 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-254 7PK - Security Features

The web-based administration console in Apache ActiveMQ 5.x before 5.13.2 does not send an X-Frame-Options HTTP header, which makes it easier for remote attackers to conduct clickjacking attacks via a crafted web page that contains a (1) FRAME or (2) IFRAME element.

- BID - 84321
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2016-0734-announcement.txt
- MLIST - [oss-security] 20160310 [ANNOUNCE] CVE-2016-0734: ActiveMQ Web Console - Clickjacking
- REDHAT - RHSA-2016:1424
- SECTRACK - 1035327

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2016-0782 suppress

Severity:Low
CVSS Score: 3.5 (AV:N/AC:M/Au:S/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

The administration web console in Apache ActiveMQ 5.x before 5.11.4, 5.12.x before 5.12.3, and 5.13.x before 5.13.2 allows remote authenticated users to conduct cross-site scripting (XSS) attacks and consequently obtain sensitive information from a Java memory dump via vectors related to creating a queue.

- BUGTRAQ - 20160310 [ANNOUNCE] CVE-2016-0782: ActiveMQ Web Console - Cross-Site Scripting
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2016-0782-announcement.txt
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1317516
- MISC - http://packetstormsecurity.com/files/136215/Apache-ActiveMQ-5.13.0-Cross-Site-Scripting.html
- REDHAT - RHSA-2016:1424
- SECTRACK - 1035328

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2016-3088 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-20 Improper Input Validation

The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.

- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2016-3088-announcement.txt
- EXPLOIT-DB - 42283
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-16-356
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-16-357
- REDHAT - RHSA-2016:2036
- SECTRACK - 1035951

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:5.13.3 and all previous versions

CVE-2016-6810 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

In Apache ActiveMQ 5.x before 5.14.2, an instance of a cross-site scripting vulnerability was identified to be present in the web based administration console. The root cause of this issue is improper user data output validation.

- BID - 94882
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2016-6810-announcement.txt
- MLIST - [users] 20161209 [ANNOUNCE] CVE-2016-6810: ActiveMQ Web Console - Cross-Site Scripting
- SECTRACK - 1037475

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

appframework-api-2.11.0.jar

Description:

API project for AppFramework

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\appframework\lib\appframework-api-2.11.0.jar
MD5: 8160235f039c205ce0c908a3319ac802
SHA1: fe6ddc3b37918788b15338be81895d75af42f06b
SHA256:b209c2fe663a42d7c62c998d3678b31162b758ae8eb48dc4e5962de7e046b8c1

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:app_project:app:2.11.0 *Confidence*:Low suppress
- **maven:** org.openmrs.module:appframework-api:2.11.0 *Confidence*:High

Published Vulnerabilities

CVE-2018-13661 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-190 Integer Overflow or Wraparound

The mintToken function of a smart contract implementation for APP, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value.

- MISC - https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md
- MISC - https://github.com/BlockChainsSecurity/EtherTokens/tree/master/APP

Vulnerable Software & Versions:

- cpe:/a:app_project:app:-

formentryapp-api-1.4.2.jar

Description:

API project for FormEntryApp

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\formentryapp\lib\formentryapp-api-1.4.2.jar
MD5: e955b5ce6f909875c821f33a866a18ce
SHA1: bdf1101deda7e8672326de45be6189162ae1c736
SHA256:d4570644b1a704d11a19ace325d28c5d5b81fac00247801abe59eb9606bbc920

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:app_project:app:1.4.2 *Confidence*:Low suppress
- **maven:** org.openmrs.module:formentryapp-api:1.4.2 *Confidence*:High

Published Vulnerabilities

CVE-2018-13661 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-190 Integer Overflow or Wraparound

The mintToken function of a smart contract implementation for APP, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value.

- MISC - https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md
- MISC - https://github.com/BlockChainsSecurity/EtherTokens/tree/master/APP

Vulnerable Software & Versions:

- cpe:/a:app_project:app:-

stax-1.2.0.jar

Description:

StAX is the reference implementation of the StAX API

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\reportingcompatibility\lib\stax-1.2.0.jar
MD5: aa3439d235f7d999532b66bac56c1f87
SHA1: c434800de5e4bbe1822805be5fb1c32d6834f830
SHA256:df6905a047b05e23bc91f03ba57ac2f87c1ddf83e048aa0e5bd13169d5ebf0d9

Evidence

Related Dependencies

Identifiers

- **maven:** stax:stax:1.2.0 ✓ *Confidence*:Highest
- **cpe:** cpe:/a:st_project:st:1.2.0 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2017-16224 suppress

Severity:Medium
CVSS Score: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)
CWE: CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

st is a module for serving static files. An attacker is able to craft a request that results in an HTTP 301 (redirect) to an entirely different domain. A request for: http://some.server.com//nodesecurity.org/%2e%2e would result in a 301 to //nodesecurity.org/%2e%2e which most browsers treat as a proper redirect as // is translated into the current schema being used. Mitigating factor: In order for this to work, st must be serving from the root of a server (/) rather than the typical sub directory (/static/) and the redirect URL will end with some form of URL encoded .. ("%2e%2e", "%2e.", ".%2e").

- MISC - https://nodesecurity.io/advisories/547

Vulnerable Software & Versions:

- cpe:/a:st_project:st:1.2.1::~~~node.js~~ and all previous versions

xstream-1.4.3.jar

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\tomcat\webapps\openmrs-standalone\WEB-INF\lib\xstream-1.4.3.jar
MD5: 8e3190161235797b8c57eda899111981
SHA1: 3427c153a5ad0f2cfa923528ad8be875c8cb1cff
SHA256:27343b2cce5c38689c1ef03d5f1c9a74812c7fca81351d29e92b1f6126730551

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:xstream_project:xstream:1.4.3 *Confidence*:Low suppress
- **maven:** com.thoughtworks.xstream:xstream:1.4.3 *Confidence*:High

Published Vulnerabilities

CVE-2016-3674 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-200 Information Exposure

Multiple XML external entity (XXE) vulnerabilities in the (1) Dom4JDriver, (2) DomDriver, (3) JDomDriver, (4) JDom2Driver, (5) SjsxpDriver, (6) StandardStaxDriver, and (7) WstxDriver drivers in XStream before 1.4.9 allow remote attackers to read arbitrary files via a crafted XML document.

- BID - 85381
- CONFIRM - http://x-stream.github.io/changes.html#1.4.9
- CONFIRM - https://github.com/x-stream/xstream/issues/25
- DEBIAN - DSA-3575
- FEDORA - FEDORA-2016-250042b8a6
- FEDORA - FEDORA-2016-de909cc333
- MLIST - [oss-security] 20160325 CVE request - XStream: XXE vulnerability
- MLIST - [oss-security] 20160328 Re: CVE request - XStream: XXE vulnerability
- REDHAT - RHSA-2016:2822
- REDHAT - RHSA-2016:2823
- SECTRACK - 1036419

Vulnerable Software & Versions:

- cpe:/a:xstream_project:xstream:1.4.8 and all previous versions

CVE-2017-7957 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-20 Improper Input Validation

XStream through 1.4.9, when a certain denyTypes workaround is not used, mishandles attempts to create an instance of the primitive type 'void' during unmarshalling, leading to a remote application crash, as demonstrated by an xstream.fromXML("<void/>") call.

- BID - 100687
- CONFIRM - http://x-stream.github.io/CVE-2017-7957.html
- CONFIRM - https://www-prd-trops.events.ibm.com/node/715749
- DEBIAN - DSA-3841
- REDHAT - RHSA-2017:1832
- REDHAT - RHSA-2017:2888
- REDHAT - RHSA-2017:2889
- SECTRACK - 1039499
- XF - xstream-cve20177957-dos(125800)

Vulnerable Software & Versions:

- cpe:/a:xstream_project:xstream:1.4.9 and all previous versions

kahadb-5.4.3.jar

Description:

An Embedded Lightweight Non-Relational Database

License:

http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\event\lib\kahadb-5.4.3.jar
MD5: ea72763fc1b57bb0bec51fc9a996ebac
SHA1: 05162743d634379204862c71fbc9880e7d619a19
SHA256:3e44fa0c333d99912f0de8ef75b870d5f60b2e360d9517fb2e2c5a6a66ff4178

Evidence

Related Dependencies

Identifiers

- **maven:** org.apache.activemq:kahadb:5.4.3 *Confidence*:High
- **cpe:** cpe:/a:apache:activemq:5.4.3 *Confidence*:Highest suppress

Published Vulnerabilities

CVE-2011-4905 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-399 Resource Management Errors

Apache ActiveMQ before 5.6.0 allows remote attackers to cause a denial of service (file-descriptor exhaustion and broker crash or hang) by sending many openwire failover:tcp:// connection requests.

- BID - 50904
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1209700
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1211844
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-3294
- MLIST - [oss-security] 20111224 CVE Request for Apache ActiveMQ DoS
- MLIST - [oss-security] 20111225 Re: CVE Request for Apache ActiveMQ DoS

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2012-5784 suppress

Severity:Medium
CVSS Score: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)
CWE: CWE-20 Improper Input Validation

Apache Axis 1.4 and earlier, as used in PayPal Payments Pro, PayPal Mass Pay, PayPal Transactional Information SOAP, the Java Message Service implementation in Apache ActiveMQ, and other products, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- BID - 56408
- MISC - http://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf
- REDHAT - RHSA-2013:0269
- REDHAT - RHSA-2013:0683

- REDHAT - RHSA-2014:0037
- XF - apache-axis-ssl-spoofing(79829)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2012-6092 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Multiple cross-site scripting (XSS) vulnerabilities in the web demos in Apache ActiveMQ before 5.8.0 allow remote attackers to inject arbitrary web script or HTML via (1) the refresh parameter to PortfolioPublishServlet.java (aka demo/portfolioPublish or Market Data Publisher), or vectors involving (2) debug logs or (3) subscribe messages in webapp/websocket/chat.js. NOTE: AMQ-4124 is covered by CVE-2012-6551.

- BID - 59400
- CONFIRM - http://activemq.apache.org/activemq-580-release.html
- CONFIRM - https://fisheye6.atlassian.com/changelog/activemq?cs=1399577
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4115
- CONFIRM - https://issues.apache.org/jira/secure/ReleaseNote.jspa?projectId=12311210&version=12323282
- REDHAT - RHSA-2013:1029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2012-6551 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-399 Resource Management Errors

The default configuration of Apache ActiveMQ before 5.8.0 enables a sample web application, which allows remote attackers to cause a denial of service (broker resource consumption) via HTTP requests.

- BID - 59401
- CONFIRM - http://activemq.apache.org/activemq-580-release.html
- CONFIRM - https://fisheye6.atlassian.com/changelog/activemq?cs=1404998
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4124
- CONFIRM - https://issues.apache.org/jira/secure/ReleaseNote.jspa?projectId=12311210&version=12323282
- MLIST - [dev] 20121022 [DISCUSS] - ActiveMQ out of the box - Should not include the demos
- REDHAT - RHSA-2013:1029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2013-1879 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in scheduled.jsp in Apache ActiveMQ 5.8.0 and earlier allows remote attackers to inject arbitrary web script or HTML via vectors involving the "cron of a message."

- BID - 61142
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4397
- REDHAT - RHSA-2013:1029
- XF - activemq-cve20131879-xss(85586)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.8.0 and all previous versions
- ...

CVE-2013-1880 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in the Portfolio publisher servlet in the demo web application in Apache ActiveMQ before 5.9.0 allows remote attackers to inject arbitrary web script or HTML via the refresh parameter to demo/portfolioPublish, a different vulnerability than CVE-2012-6092.

- BID - 65615
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=924447
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4398
- REDHAT - RHSA-2013:1029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.8.0 and all previous versions
- ...

CVE-2013-3060 suppress

Severity:Medium
CVSS Score: 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)
CWE: CWE-287 Improper Authentication

The web console in Apache ActiveMQ before 5.8.0 does not require authentication, which allows remote attackers to obtain sensitive information or cause a denial of service via HTTP requests.

- BID - 59402
- CONFIRM - http://activemq.apache.org/activemq-580-release.html
- CONFIRM - https://fisheye6.atlassian.com/changelog/activemq?cs=1404998
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4124
- CONFIRM - https://issues.apache.org/jira/secure/ReleaseNote.jspa?projectId=12311210&version=12323282
- MLIST - [dev] 20121022 [DISCUSS] - ActiveMQ out of the box - Should not include the demos
- REDHAT - RHSA-2013:1029
- REDHAT - RHSA-2013:1221

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2014-3576 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

The processControlCommand function in broker/TransportConnection.java in Apache ActiveMQ before 5.11.0 allows remote attackers to cause a denial of service (shutdown) via a shutdown command.

- BID - 76272
- BUGTRAQ - 20151106 [ANNOUNCE] CVE-2014-3576 - Apache ActiveMQ vulnerabilities
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
- CONFIRM - https://github.com/apache/activemq/commit/00921f2
- DEBIAN - DSA-3330
- MISC - http://packetstormsecurity.com/files/134274/Apache-ActiveMQ-5.10.1-Denial-Of-Service.html
- MLIST - [dev] 20150721 About CVE-2014-3576
- SECTRACK - 1033898

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.10.0 and all previous versions
- ...

CVE-2014-3600 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-611 Improper Restriction of XML External Entity Reference ('XXE')

XML external entity (XXE) vulnerability in Apache ActiveMQ 5.x before 5.10.1 allows remote consumers to have unspecified impact via vectors involving an XPath based selector when dequeuing XML messages.

- BID - 72510
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2014-3600-announcement.txt
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-5333
- MLIST - [oss-security] 20150205 [ANNOUNCE] CVE-2014-3600, CVE-2014-3612 and CVE-2014-8110 - Apache ActiveMQ vulnerabilities
- XF - apache-activemq-cve20143600-info-disc(100722)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2014-3612 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-287 Improper Authentication

The LDAPLoginModule implementation in the Java Authentication and Authorization Service (JAAS) in Apache ActiveMQ 5.x before 5.10.1 allows remote attackers to bypass authentication by logging in with an empty password and valid username, which triggers an unauthenticated bind. NOTE: this identifier has been SPLIT per ADT2 due to different vulnerability types. See CVE-2015-6524 for the use of wildcard operators in usernames.

- BID - 72513
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2014-3612-announcement.txt
- MLIST - [oss-security] 20150205 [ANNOUNCE] CVE-2014-3600, CVE-2014-3612 and CVE-2014-8110 - Apache ActiveMQ vulnerabilities
- REDHAT - RHSA-2015:0137
- REDHAT - RHSA-2015:0138

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2014-8110 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Multiple cross-site scripting (XSS) vulnerabilities in the web based administration console in Apache ActiveMQ 5.x before 5.10.1 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- BID - 72511
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2014-8110-announcement.txt
- MLIST - [oss-security] 20150205 [ANNOUNCE] CVE-2014-3600, CVE-2014-3612 and CVE-2014-8110 - Apache ActiveMQ vulnerabilities
- XF - apache-activemq-cve20148110-xss(100724)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2015-1830 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Directory traversal vulnerability in the fileserver upload/download functionality for blob messages in Apache ActiveMQ 5.x before 5.11.2 for Windows allows remote attackers to create JSP files in arbitrary directories via unspecified vectors.

- BID - 76452
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2015-1830-announcement.txt
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-15-407
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-15-407/
- SECTRACK - 1033315

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2015-5182 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-352 Cross-Site Request Forgery (CSRF)

Cross-site request forgery (CSRF) vulnerability in the jolokia API in A-MQ.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1248809

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:-

CVE-2015-5183 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-254 7PK - Security Features

The Hawtio console in A-MQ does not set HTTPOnly or Secure attributes on cookies.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1249182

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:-

CVE-2015-5184 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-254 7PK - Security Features

The Hawtio console in A-MQ allows remote attackers to obtain sensitive information and perform other unspecified impact.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1249183

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:-

CVE-2015-5254 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-20 Improper Input Validation

Apache ActiveMQ 5.x before 5.13.0 does not restrict the classes that can be serialized in the broker, which allows remote attackers to execute arbitrary code via a crafted serialized Java Message Service (JMS) ObjectMessage object.

- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2015-5254-announcement.txt
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05385680
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-6013
- DEBIAN - DSA-3524
- FEDORA - FEDORA-2015-7ca4368b0c
- FEDORA - FEDORA-2015-eefc5a6762
- MLIST - [oss-security] 20151208 [ANNOUNCE] CVE-2015-5254 - Unsafe deserialization in ActiveMQ
- REDHAT - RHSA-2016:0489
- REDHAT - RHSA-2016:2035
- REDHAT - RHSA-2016:2036

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2015-6524 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-255 Credentials Management

The LDAPLoginModule implementation in the Java Authentication and Authorization Service (JAAS) in Apache ActiveMQ 5.x before 5.10.1 allows wildcard operators in usernames, which allows remote attackers to obtain credentials via a brute force attack. NOTE: this identifier was SPLIT from CVE-2014-3612 per ADT2 due to different vulnerability types.

- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2014-3612-announcement.txt
- FEDORA - FEDORA-2015-5622085024

- FEDORA - FEDORA-2015-701a1e1a5f

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2016-0734 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-254 7PK - Security Features

The web-based administration console in Apache ActiveMQ 5.x before 5.13.2 does not send an X-Frame-Options HTTP header, which makes it easier for remote attackers to conduct clickjacking attacks via a crafted web page that contains a (1) FRAME or (2) IFRAME element.

- BID - 84321
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2016-0734-announcement.txt
- MLIST - [oss-security] 20160310 [ANNOUNCE] CVE-2016-0734: ActiveMQ Web Console - Clickjacking
- REDHAT - RHSA-2016:1424
- SECTRACK - 1035327

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2016-0782 suppress

Severity:Low
CVSS Score: 3.5 (AV:N/AC:M/Au:S/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

The administration web console in Apache ActiveMQ 5.x before 5.11.4, 5.12.x before 5.12.3, and 5.13.x before 5.13.2 allows remote authenticated users to conduct cross-site scripting (XSS) attacks and consequently obtain sensitive information from a Java memory dump via vectors related to creating a queue.

- BUGTRAQ - 20160310 [ANNOUNCE] CVE-2016-0782: ActiveMQ Web Console - Cross-Site Scripting
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2016-0782-announcement.txt
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1317516
- MISC - http://packetstormsecurity.com/files/136215/Apache-ActiveMQ-5.13.0-Cross-Site-Scripting.html
- REDHAT - RHSA-2016:1424
- SECTRACK - 1035328

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

CVE-2016-3088 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-20 Improper Input Validation

The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.

- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2016-3088-announcement.txt
- EXPLOIT-DB - 42283
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-16-356
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-16-357
- REDHAT - RHSA-2016:2036
- SECTRACK - 1035951

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:5.13.3 and all previous versions

CVE-2016-6810 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

In Apache ActiveMQ 5.x before 5.14.2, an instance of a cross-site scripting vulnerability was identified to be present in the web based administration console. The root cause of this issue is improper user data output validation.

- BID - 94882
- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2016-6810-announcement.txt
- MLIST - [users] 20161209 [ANNOUNCE] CVE-2016-6810: ActiveMQ Web Console - Cross-Site Scripting
- SECTRACK - 1037475

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.4.3
- ...

httpclient-4.2.jar

Description:

HttpComponents Client (base module)

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\idgen\lib\httpclient-4.2.jar
MD5: c16abd2428d2abf95e0af53aaa775f1b
SHA1: 894b77b74ac06206075bccc22868ef83d69e383b
SHA256:7a1791f3ef17acfb75d4c6a3e124b9a96946e02e2381e3f59f5bc500a7607208

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:apache:httpclient:4.2 *Confidence*:Highest suppress
- **maven:** org.apache.httpcomponents:httpclient:4.2 *Confidence*:High

Published Vulnerabilities

CVE-2014-3577 suppress

Severity:Medium
CVSS Score: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

org.apache.http.conn.ssl.AbstractVerifier in Apache HttpComponents HttpClient before 4.3.5 and HttpAsyncClient before 4.0.2 does not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a "CN=" string in a field in the distinguished name (DN) of a certificate, as demonstrated by the "foo,CN=www.apache.org" string in the O field.

- BID - 69258
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://access.redhat.com/solutions/1165533
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05103564
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05363782
- FULLDISC - 20140818 CVE-2014-3577: Apache HttpComponents client: Hostname verification susceptible to MITM attack
- MISC - http://packetstormsecurity.com/files/127913/Apache-HttpComponents-Man-In-The-Middle.html
- OSVDB - 110143
- REDHAT - RHSA-2014:1146
- REDHAT - RHSA-2014:1166
- REDHAT - RHSA-2014:1833
- REDHAT - RHSA-2014:1834
- REDHAT - RHSA-2014:1835
- REDHAT - RHSA-2014:1836
- REDHAT - RHSA-2014:1891
- REDHAT - RHSA-2014:1892
- REDHAT - RHSA-2015:0125
- REDHAT - RHSA-2015:0158
- REDHAT - RHSA-2015:0675
- REDHAT - RHSA-2015:0720
- REDHAT - RHSA-2015:0765
- REDHAT - RHSA-2015:0850
- REDHAT - RHSA-2015:0851
- REDHAT - RHSA-2015:1176
- REDHAT - RHSA-2015:1177
- REDHAT - RHSA-2015:1888
- REDHAT - RHSA-2016:1773
- REDHAT - RHSA-2016:1931
- SECTRACK - 1030812
- SECUNIA - 60466
- UBUNTU - USN-2769-1
- XF - apache-cve20143577-spoofing(95327)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:httpclient:4.2:alpha1
- ...

hadoop-auth-2.2.0.jar

Description:

Apache Hadoop Auth - Java HTTP SPNEGO

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\chartsearch\lib\hadoop-auth-2.2.0.jar
MD5: 8bb0f03bea387738b61642a2502b3289
SHA1: 74e5f8b2134be51312c004d29e33a7bf4377ce20
SHA256:f2c50d66e049c378088975774656d8e111265d12fbba1cde97de71dd01b96d2b

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:apache:hadoop:2.2.0 *Confidence*:Highest suppress
- **maven:** org.apache.hadoop:hadoop-auth:2.2.0 *Confidence*:High

Published Vulnerabilities

CVE-2014-0229 suppress

Severity:Medium
CVSS Score: 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

Apache Hadoop 0.23.x before 0.23.11 and 2.x before 2.4.1, as used in Cloudera CDH 5.0.x before 5.0.2, do not check authorization for the (1) refreshNamenodes, (2) deleteBlockPool, and (3) shutdownDatanode HDFS admin commands, which allows remote authenticated users to cause a denial of service (DataNodes shutdown) or perform unnecessary operations by issuing a command.

- CONFIRM - https://www.cloudera.com/documentation/other/security-bulletins/topics/csb_topic_1.html#concept_i1q_xvk_2r

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:hadoop:2.2.0
- ...

CVE-2014-3627 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-59 Improper Link Resolution Before File Access ('Link Following')

The YARN NodeManager daemon in Apache Hadoop 0.23.0 through 0.23.11 and 2.x before 2.5.2, when using Kerberos authentication, allows remote cluster users to change the permissions of certain files to world-readable via a symlink attack in a public tar archive, which is not properly handled during localization, related to distributed cache.

- MLIST - [hadoop-general] 20141121 [ANNOUNCE] Apache Hadoop 2.5.2 released

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:hadoop:2.2.0
- ...

CVE-2016-5001 suppress

Severity:Low
CVSS Score: 2.1 (AV:L/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-200 Information Exposure

This is an information disclosure vulnerability in Apache Hadoop before 2.6.4 and 2.7.x before 2.7.2 in the short-circuit reads feature of HDFS. A local user on an HDFS DataNode may be able to craft a block token that grants unauthorized read access to random files by guessing certain fields in the token.

- BID - 94950
- MLIST - [oss-security] 20161216 [SECURITY] CVE-2016-5001: Apache Hadoop Information Disclosure

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:hadoop:2.6.3 and all previous versions
- ...

CVE-2016-6811 suppress

Severity:High
CVSS Score: 9.0 (AV:N/AC:L/Au:S/C:C/I:C/A:C)
CWE: CWE-264 Permissions, Privileges, and Access Controls

In Apache Hadoop 2.x before 2.7.4, a user who can escalate to yarn user can possibly run arbitrary commands as root user.

- MLIST - [general] 20180501 CVE-2016-6811: Apache Hadoop Privilege escalation vulnerability

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:hadoop:2.2.0
- ...

CVE-2017-15713 suppress

Severity:Medium
CVSS Score: 4.0 (AV:N/AC:L/Au:S/C:P/I:N/A:N)
CWE: CWE-200 Information Exposure

Vulnerability in Apache Hadoop 0.23.x, 2.x before 2.7.5, 2.8.x before 2.8.3, and 3.0.0-alpha through 3.0.0-beta1 allows a cluster user to expose private files owned by the user running the MapReduce job history server process. The malicious user can construct a configuration file containing XML directives that reference sensitive files on the MapReduce job history server host.

- MLIST - [general] 20180119 CVE-2017-15713: Apache Hadoop MapReduce job history server vulnerability

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:hadoop:2.2.0
- ...

CVE-2017-3161 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

The HDFS web UI in Apache Hadoop before 2.7.0 is vulnerable to a cross-site scripting (XSS) attack through an unescaped query parameter.

- BID - 98025
- MLIST - [hadoop-common-dev] 20170425 CVE-2017-3161: Apache Hadoop NameNode XSS vulnerability

Vulnerable Software & Versions:

- cpe:/a:apache:hadoop:2.6.5 and all previous versions

CVE-2017-3162 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-20 Improper Input Validation

HDFS clients interact with a servlet on the DataNode to browse the HDFS namespace. The NameNode is provided as a query parameter that is not validated in Apache Hadoop before 2.7.0.

- BID - 98017
- MLIST - [hadoop-common-dev] 20170425 CVE-2017-3162: Apache Hadoop DataNode web UI vulnerability

Vulnerable Software & Versions:

- cpe:/a:apache:hadoop:2.6.5 and all previous versions

protobuf-java-2.5.0.jar

Description:

Protocol Buffers are a way of encoding structured data in an efficient yet extensible format.

License:

New BSD license: http://www.opensource.org/licenses/bsd-license.php

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\chartsearch\lib\protobuf-java-2.5.0.jar
MD5: a44473b98947e2a54c54e0db1387d137
SHA1: a10732c76bfacdbd633a7eb0f7968b1059a65dfa
SHA256:e0c1c64575c005601725e7c6a02cebf9e1285e888f756b2a1d73ffa8d725cc74

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:google:protobuf:2.5.0 *Confidence*:Highest suppress
- **maven:** com.google.protobuf:protobuf-java:2.5.0 *Confidence*:High

Published Vulnerabilities

CVE-2015-5237 suppress

Severity:Medium
CVSS Score: 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)
CWE: CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

protobuf allows remote authenticated attackers to cause a heap-based buffer overflow.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1256426
- CONFIRM - https://github.com/google/protobuf/issues/760
- MLIST - [oss-security] 20150827 CVE-2015-5237: Integer overflow in protobuf serialization (currently minor)

Vulnerable Software & Versions: (show all)

- cpe:/a:google:protobuf:2.5.0
- ...

commons-beanutils-1.7.0.jar

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\tomcat\webapps\openmrs-standalone\WEB-INF\lib\commons-beanutils-1.7.0.jar
MD5: 0f18acf5fa857f9959675e14d901a7ce
SHA1: 5675fd96b29656504b86029551973d60fb41339b
SHA256:24bcaa20ccbdc7c856ce0c0aea144566943403e2e9f27bd9779cda1d76823ef4

Evidence

Related Dependencies

Identifiers

- **maven:** commons-beanutils:commons-beanutils:1.7.0 ✓ *Confidence*:Highest
- **cpe:** cpe:/a:apache:commons_beanutils:1.7.0 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2014-0114 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-20 Improper Input Validation

Apache Commons BeanUtils, as distributed in lib/commons-beanutils-1.8.0.jar in Apache Struts 1.x through 1.3.10 and in other products requiring commons-beanutils through 1.9.2, does not suppress the class property, which allows remote attackers to "manipulate" the ClassLoader and execute arbitrary code via the class parameter, as demonstrated by the passing of this parameter to the getClass method of the ActionForm object in Struts 1.

- BID - 67121
- BUGTRAQ - 20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
- CONFIRM - http://advisories.mageia.org/MGASA-2014-0219.html
- CONFIRM - http://commons.apache.org/proper/commons-beanutils/javadocs/v1.9.2/RELEASE-NOTES.txt
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21674128
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21674812
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675266
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675387
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675689
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675898
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675972
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676091
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676110
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676303
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676375
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676931
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21677110
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg27042296
- CONFIRM - http://www.ibm.com/support/docview.wss?uid=swg21675496
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
- CONFIRM - http://www.vmware.com/security/advisories/VMSA-2014-0008.html
- CONFIRM - http://www.vmware.com/security/advisories/VMSA-2014-0012.html
- CONFIRM - https://access.redhat.com/solutions/869353
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1091938
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1116665
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05324755
- CONFIRM - https://issues.apache.org/jira/browse/BEANUTILS-463
- CONFIRM - https://security.netapp.com/advisory/ntap-20140911-0001/
- CONFIRM - https://security.netapp.com/advisory/ntap-20180629-0006/
- DEBIAN - DSA-2940
- FEDORA - FEDORA-2014-9380
- FULLDISC - 20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
- GENTOO - GLSA-201607-09
- HP - HPSBGN03041
- HP - HPSBMU03090
- HP - HPSBST03160
- MANDRIVA - MDVSA-2014:095
- MLIST - [apache-ignite-developers] 20180601 [CVE-2014-0114]: Apache Ignite is vulnerable to existing CVE-2014-0114
- MLIST - [oss-security] 20140616 CVE request for commons-beanutils: 'class' property is exposed, potentially leading to RCE
- MLIST - [oss-security] 20140707 Re: CVE request for commons-beanutils: 'class' property is exposed, potentially leading to RCE
- SECUNIA - 57477
- SECUNIA - 58710
- SECUNIA - 58947
- SECUNIA - 59118
- SECUNIA - 59228
- SECUNIA - 59245
- SECUNIA - 59246
- SECUNIA - 59430
- SECUNIA - 59464
- SECUNIA - 59479
- SECUNIA - 59480

- SECUNIA - 59718

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:commons_beanutils:1.9.1 and all previous versions
- ...

jasypt-1.6.jar

Description:

Java library which enables encryption in java apps with minimum effort.

License:

The Apache Software License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\event\lib\jasypt-1.6.jar
MD5: 1c83fe6d7a403b7361914ea065e848ba
SHA1: 1550a512e10a517a557254f15a12392393245610
SHA256:2736c5b355f14141dc32c03796f5c19273578b9ca3f0bf7630e8ba5ef379a150

Evidence

Related Dependencies

Identifiers

- **maven:** org.jasypt:jasypt:1.6 *Confidence*:High
- **cpe:** cpe:/a:jasypt_project:jasypt:1.6 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2014-9970 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-200 Information Exposure

jasypt before 1.9.2 allows a timing attack against the password hash comparison.

- CONFIRM - https://sourceforge.net/p/jasypt/code/668/
- REDHAT - RHSA-2017:2546
- REDHAT - RHSA-2017:2547
- REDHAT - RHSA-2017:2808
- REDHAT - RHSA-2017:2809
- REDHAT - RHSA-2017:2810
- REDHAT - RHSA-2017:2811
- REDHAT - RHSA-2017:3141
- REDHAT - RHSA-2018:0294
- SECTRACK - 1039744
- SECTRACK - 1040360

Vulnerable Software & Versions:

- cpe:/a:jasypt_project:jasypt:1.9.1 and all previous versions

mysql-connector-java-5.1.28.jar

Description:

MySQL JDBC Type 4 driver

License:

The GNU General Public License, Version 2: http://www.gnu.org/licenses/old-licenses/gpl-2.0.html

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\tomcat\webapps\openmrs-standalone\WEB-INF\lib\mysql-connector-java-5.1.28.jar
MD5: 18cdffd712f897296a5623c448448f7b
SHA1: 4c3e03dd2c60b8975ed68f72aa18229db2647196
SHA256:9e69233253d9c6d9e232636bea0b74dc15ab5f9e216087de0a3d1f09f8f0992c

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:oracle:mysql:5.1.28 *Confidence*:Low suppress
- **maven:** mysql:mysql-connector-java:5.1.28 ✓ *Confidence*:Highest
- **cpe:** cpe:/a:mysql:mysql:5.1.28 *Confidence*:Highest suppress
- **cpe:** cpe:/a:oracle:mysql_connectors:5.1.28 *Confidence*:Low suppress
- **cpe:** cpe:/a:sun:mysql_connector/j:5.1.28 *Confidence*:Low suppress
- **cpe:** cpe:/a:oracle:connector/j:5.1.28 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2017-3523 suppress

Severity:Medium
CVSS Score: 6.0 (AV:N/AC:M/Au:S/C:P/I:P/A:P)
CWE: CWE-284 Improper Access Control

Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J). Supported versions that are affected are 5.1.40 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. While the vulnerability is in MySQL Connectors, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.0 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).

- BID - 97982
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
- DEBIAN - DSA-3840

Vulnerable Software & Versions: (show all)

- cpe:/a:oracle:connector/j:5.1.40 and all previous versions
- ...

CVE-2017-3586 suppress

Severity:Medium
CVSS Score: 5.5 (AV:N/AC:L/Au:S/C:P/I:P/A:N)
CWE: CWE-284 Improper Access Control

Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J). Supported versions that are affected are 5.1.41 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. While the vulnerability is in MySQL Connectors, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data as well as unauthorized read access to a subset of MySQL Connectors accessible data. CVSS 3.0 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N).

- BID - 97784
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
- DEBIAN - DSA-3857
- SECTRACK - 1038287

Vulnerable Software & Versions:

- cpe:/a:oracle:mysql_connectors:5.1.41 and all previous versions

CVE-2017-3589 suppress

Severity:Low
CVSS Score: 2.1 (AV:L/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-284 Improper Access Control

Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J). Supported versions that are affected are 5.1.41 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Connectors executes to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data. CVSS 3.0 Base Score 3.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

- BID - 97836
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
- DEBIAN - DSA-3857
- SECTRACK - 1038287

Vulnerable Software & Versions: (show all)

- cpe:/a:oracle:connector/j:5.1.41 and all previous versions
- ...

CVE-2018-3081 suppress

Severity:Medium
CVSS Score: 4.9 (AV:N/AC:M/Au:S/C:N/I:P/A:P)
CWE: CWE-284 Improper Access Control

Vulnerability in the MySQL Client component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client as well as unauthorized update, insert or delete access to some of MySQL Client accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).

- BID - 104779
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://security.netapp.com/advisory/ntap-20180726-0002/

- SECTRACK - 1041294
- UBUNTU - USN-3725-1
- UBUNTU - USN-3725-2

Vulnerable Software & Versions: (show all)

- cpe:/a:oracle:mysql:5.5.60 and all previous versions
- ...

zookeeper-3.4.6.jar

License:

http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\chartsearch\lib\zookeeper-3.4.6.jar
MD5: 7d01d317c717268725896cfb81b18152
SHA1: 01b2502e29da1ebaade2357cd1de35a855fa3755
SHA256:8a375a1ef98cbc0e1f6e9dfd0d96d914b74d37ad00b4bf81beb77fa8f34d33ae

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:apache:zookeeper:3.4.6 *Confidence*:Highest suppress
- **maven:** org.apache.zookeeper:zookeeper:3.4.6 ✓ *Confidence*:Highest

Published Vulnerabilities

CVE-2014-0085 suppress

Severity:Low
CVSS Score: 2.1 (AV:L/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-255 Credentials Management

JBoss Fuse did not enable encrypted passwords by default in its usage of Apache Zookeeper. This permitted sensitive information disclosure via logging to local users. Note: this description has been updated; previous text mistakenly identified the source of the flaw as Zookeeper. Previous text: Apache Zookeeper logs cleartext admin passwords, which allows local users to obtain sensitive information by reading the log.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-0085

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:zookeeper:-
- ...

CVE-2016-5017 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

Buffer overflow in the C cli shell in Apache Zookeeper before 3.4.9 and 3.5.x before 3.5.3, when using the "cmd:" batch mode syntax, allows attackers to have unspecified impact via a long command string.

- BID - 93044
- CONFIRM - https://git-wip-us.apache.org/repos/asf?p=zookeeper.git;a=commitdiff;h=27ecf981a15554dc8e64a28630af7a5c9e2bdf4f
- CONFIRM - https://git-wip-us.apache.org/repos/asf?p=zookeeper.git;a=commitdiff;h=f09154d6648eeb4ec5e1ac8a2bacbd2f8c87c14a
- CONFIRM - https://www.cloudera.com/documentation/other/security-bulletins/topics/csb_topic_1.html
- CONFIRM - https://zookeeper.apache.org/security.html#CVE-2016-5017
- MISC - http://packetstormsecurity.com/files/138755/ZooKeeper-3.4.8-3.5.2-Buffer-Overflow.html
- MLIST - [oss-security] 20160916 [SECURITY] CVE-2016-5017: Buffer overflow vulnerability in ZooKeeper C cli shell

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:zookeeper:3.4.8 and all previous versions
- ...

CVE-2017-5637 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-399 Resource Management Errors

Two four letter word commands "wchp/wchc" are CPU intensive and could cause spike of CPU utilization on Apache ZooKeeper server if abused, which leads to the server unable to serve legitimate client requests. Apache ZooKeeper thru version 3.4.9 and 3.5.2 suffer from this issue, fixed in 3.4.10, 3.5.3, and later.

- BID - 98814
- CONFIRM - https://issues.apache.org/jira/browse/ZOOKEEPER-2693
- DEBIAN - DSA-3871

- MLIST - [dev] 20171009 [SECURITY] CVE-2017-5637: DOS attack on wchp/wchc four letter words (4lw)
- REDHAT - RHSA-2017:2477
- REDHAT - RHSA-2017:3354
- REDHAT - RHSA-2017:3355

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:zookeeper:3.4.6
- ...

CVE-2018-8012 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-285 Improper Authorization

No authentication/authorization is enforced when a server attempts to join a quorum in Apache ZooKeeper before 3.4.10, and 3.5.0-alpha through 3.5.3-beta. As a result an arbitrary end point could join the cluster and begin propagating counterfeit changes to the leader.

- BID - 104253
- DEBIAN - DSA-4214
- MISC - https://lists.apache.org/thread.html/c75147028c1c79bdebd4f8fa5db2b77da85de2b05ecc0d54d708b393@%3Cdev.zookeeper.apache.org%3E
- SECTRACK - 1040948

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:zookeeper:-
- ...

standard-1.1.2.jar

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\tomcat\webapps\openmrs-standalone\WEB-INF\lib\standard-1.1.2.jar
MD5: 65351d0487ad57edda9171bb3b46b98c
SHA1: a17e8a4d9a1f7fcc5eed606721c9ed6b7f18acf7
SHA256:2c0048ab3ce75a202f692b159d6aa0a68edce3e4e4c5123a3359a38b29faa6b1

Evidence

Related Dependencies

Identifiers

- **maven:** taglibs:standard:1.1.2 ✓ *Confidence*:Highest
- **cpe:** cpe:/a:apache:standard_taglibs:1.1.2 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2015-0254 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Apache Standard Taglibs before 1.2.3 allows remote attackers to execute arbitrary code or conduct external XML entity (XXE) attacks via a crafted XSLT extension in a (1) <x:parse> or (2) <x:transform> JSTL XML tag.

- BID - 72809
- BUGTRAQ - 20150227 [SECURITY] CVE-2015-0254 XXE and RCE via XSL extension in JSTL XML tags
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
- MISC - http://packetstormsecurity.com/files/130575/Apache-Standard-Taglibs-1.2.1-XXE-Remote-Command-Execution.html
- MLIST - [tomcat-taglibs-user] 20150227 [SECURITY] CVE-2015-0254 XXE and RCE via XSL extension in JSTL XML tags
- REDHAT - RHSA-2015:1695
- REDHAT - RHSA-2016:1376
- REDHAT - RHSA-2016:1838
- REDHAT - RHSA-2016:1839
- REDHAT - RHSA-2016:1840
- REDHAT - RHSA-2016:1841
- SECTRACK - 1034934
- SUSE - openSUSE-SU-2015:1751
- UBUNTU - USN-2551-1

Vulnerable Software & Versions:

- cpe:/a:apache:standard_taglibs:1.2.1 and all previous versions

commons-fileupload-1.2.1.jar

Description:

The FileUpload component provides a simple yet flexible means of adding support for multipart file upload functionality to servlets and web applications.

License:

http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\chartsearch\lib\commons-fileupload-1.2.1.jar
MD5: 951b36984148fc4f4e901f06ab382273
SHA1: 384faa82e193d4e4b0546059ca09572654bc3970
SHA256:47f63b9b2c66f467b9d40cb3c3e4364a74eb6578a6e9cc145c2df3c3e65f9472

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:apache:commons_fileupload:1.2.1 *Confidence*:Highest suppress
- **maven:** commons-fileupload:commons-fileupload:1.2.1 *Confidence*:High

Published Vulnerabilities

CVE-2013-0248 suppress

Severity:Low
CVSS Score: 3.3 (AV:L/AC:M/Au:N/C:N/I:P/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

The default configuration of javax.servlet.context.tempdir in Apache Commons FileUpload 1.0 through 1.2.2 uses the /tmp directory for uploaded files, which allows local users to overwrite arbitrary files via an unspecified symlink attack.

- BID - 58326
- BUGTRAQ - 20130306 [SECURITY] CVE-2013-0248 Apache Commons FileUpload - Insecure examples
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- HP - HPSBMU03409

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:commons_fileupload:1.2.1
- ...

CVE-2014-0050 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

MultipartStream.java in Apache Commons FileUpload before 1.3.1, as used in Apache Tomcat, JBoss Web, and other products, allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted Content-Type header that bypasses a loop's intended exit conditions.

- BID - 65400
- BUGTRAQ - 20140625 NEW VMSA-2014-0007 - VMware product updates address security vulnerabilities in Apache Struts library
- BUGTRAQ - 20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
- CONFIRM - http://advisories.mageia.org/MGASA-2014-0110.html
- CONFIRM - http://svn.apache.org/r1565143
- CONFIRM - http://tomcat.apache.org/security-7.html
- CONFIRM - http://tomcat.apache.org/security-8.html
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21669554
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675432
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676091
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676092
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676401
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676403
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676405
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676410
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676656
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676853
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21677691
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21677724
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21681214
- CONFIRM - http://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/HS14-015/index.html
- CONFIRM - http://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/HS14-016/index.html
- CONFIRM - http://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/HS14-017/index.html
- CONFIRM - http://www.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-350733.htm
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html

- CONFIRM - http://www.vmware.com/security/advisories/VMSA-2014-0007.html
- CONFIRM - http://www.vmware.com/security/advisories/VMSA-2014-0008.html
- CONFIRM - http://www.vmware.com/security/advisories/VMSA-2014-0012.html
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1062337
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05324755
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05376917
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
- DEBIAN - DSA-2856
- FULLDISC - 20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
- HP - HPSBGN03329
- JVN - JVN#14876762
- JVNDB - JVNDB-2014-000017
- MANDRIVA - MDVSA-2015:084
- MISC - http://blog.spiderlabs.com/2014/02/cve-2014-0050-exploit-with-boundaries-loops-without-boundaries.html
- MISC - http://packetstormsecurity.com/files/127215/VMware-Security-Advisory-2014-0007.html
- MLIST - [commons-dev] 20140206 [SECURITY] CVE-2014-0050 Apache Commons FileUpload and Apache Tomcat DoS
- REDHAT - RHSA-2014:0252
- REDHAT - RHSA-2014:0253
- REDHAT - RHSA-2014:0400
- UBUNTU - USN-2130-1

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:commons_fileupload:1.2.1
- ...

CVE-2016-1000031 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-284 Improper Access Control

Apache Commons FileUpload before 1.3.3 DiskFileItem File Manipulation Remote Code Execution

- BID - 93604
- CONFIRM - https://issues.apache.org/jira/browse/FILEUPLOAD-279
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-16-570/
- MISC - https://www.tenable.com/security/research/tra-2016-12
- MISC - https://www.tenable.com/security/research/tra-2016-23
- MISC - https://www.tenable.com/security/research/tra-2016-30

Vulnerable Software & Versions:

- cpe:/a:apache:commons_fileupload:1.3.2 and all previous versions

CVE-2016-3092 suppress

Severity:High
CVSS Score: 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
CWE: CWE-20 Improper Input Validation

The MultipartStream class in Apache Commons Fileupload before 1.3.2, as used in Apache Tomcat 7.x before 7.0.70, 8.x before 8.0.36, 8.5.x before 8.5.3, and 9.x before 9.0.0.M7 and other products, allows remote attackers to cause a denial of service (CPU consumption) via a long boundary string.

- BID - 91453
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1743480
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1743722
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1743738
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1743742
- CONFIRM - http://tomcat.apache.org/security-7.html
- CONFIRM - http://tomcat.apache.org/security-8.html
- CONFIRM - http://tomcat.apache.org/security-9.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/bulletinjul2016-3090568.html
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1349468
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05204371
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05289840
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05324759
- DEBIAN - DSA-3609
- DEBIAN - DSA-3611
- DEBIAN - DSA-3614
- GENTOO - GLSA-201705-09
- JVN - JVN#89379547
- JVNDB - JVNDB-2016-000121
- MLIST - [dev] 20160621 CVE-2016-3092: Apache Commons Fileupload information disclosure vulnerability
- REDHAT - RHSA-2016:2068
- REDHAT - RHSA-2016:2069
- REDHAT - RHSA-2016:2070
- REDHAT - RHSA-2016:2071
- REDHAT - RHSA-2016:2072
- REDHAT - RHSA-2016:2599
- REDHAT - RHSA-2016:2807
- REDHAT - RHSA-2016:2808
- REDHAT - RHSA-2017:0455
- REDHAT - RHSA-2017:0456
- REDHAT - RHSA-2017:0457
- SECTRACK - 1036427
- SECTRACK - 1036900
- SECTRACK - 1037029
- SECTRACK - 1039606
- SUSE - openSUSE-SU-2016:2252
- UBUNTU - USN-3024-1
- UBUNTU - USN-3027-1

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:commons_fileupload:1.3.1 and all previous versions
- ...

chartsearch-api-2.1.0.jar

Description:

API project for ChartSearch

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\chartsearch\lib\chartsearch-api-2.1.0.jar
MD5: 19425e59e426f5d5426ac36a7c3c23a7
SHA1: eebd72cffd5dc05b6ba62eca24934b04c50c2074
SHA256:43b8b0da33650c6a385372461466eab92f1e5760bcf77e8ca046ceae483af4ca

Evidence

Related Dependencies

Identifiers

- **maven:** org.openmrs.module:chartsearch-api:2.1.0 *Confidence*:High
- **cpe:** cpe:/a:openmrs:openmrs:2.1::~~standalone~~~ *Confidence*:Highest suppress

Published Vulnerabilities

CVE-2014-8071 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Multiple cross-site scripting (XSS) vulnerabilities in OpenMRS 2.1 Standalone Edition allow remote attackers to inject arbitrary web script or HTML via the (1) givenName, (2) familyName, (3) address1, or (4) address2 parameter to registrationapp/registerPatient.page; the (5) comment parameter to allergyui/allergy.page; the (6) w10 parameter to htmlformentryui/htmlform/enterHtmlForm/submit.action; the (7) HTTP Referer Header to login.htm; the (8) returnUrl parameter to htmlformentryui/htmlform/enterHtmlFormWithStandardUi.page or (9) coreapps/mergeVisits.page; or the (10) visitId parameter to htmlformentryui/htmlform/enterHtmlFormWithSimpleUi.page.

- BID - 70664
- MISC - http://packetstormsecurity.com/files/128748/OpenMRS-2.1-Access-Bypass-XSS-CSRF.html
- XF - openmrs-cve20148071-xss(97690)

Vulnerable Software & Versions:

- cpe:/a:openmrs:openmrs:2.1::~~standalone~~~

CVE-2014-8072 suppress

Severity:Medium
CVSS Score: 4.0 (AV:N/AC:L/Au:S/C:P/I:N/A:N)
CWE: CWE-264 Permissions, Privileges, and Access Controls

The administration module in OpenMRS 2.1 Standalone Edition allows remote authenticated users to obtain read access via a direct request to /admin.

- BID - 70664
- MISC - http://packetstormsecurity.com/files/128748/OpenMRS-2.1-Access-Bypass-XSS-CSRF.html
- XF - openmrs-cve20148072-access-bypass(97693)

Vulnerable Software & Versions:

- cpe:/a:openmrs:openmrs:2.1::~~standalone~~~

CVE-2014-8073 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-352 Cross-Site Request Forgery (CSRF)

Cross-site request forgery (CSRF) vulnerability in OpenMRS 2.1 Standalone Edition allows remote attackers to hijack the authentication of administrators for requests that add a new user via a Save User action to admin/users/user.form.

- BID - 70664
- MISC - http://packetstormsecurity.com/files/128748/OpenMRS-2.1-Access-Bypass-XSS-CSRF.html
- XF - openmrs-cve20148073-csrf(97692)

Vulnerable Software & Versions:

- cpe:/a:openmrs:openmrs:2.1::~~standalone~~~

CVE-2017-12796 suppress

Severity:High
CVSS Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
CWE: CWE-502 Deserialization of Untrusted Data

The Reporting Compatibility Add On before 2.0.4 for OpenMRS, as distributed in OpenMRS Reference Application before 2.6.1, does not authenticate users when deserializing XML input into ReportSchema objects. The result is that remote unauthenticated users are able to execute operating system commands by crafting malicious XML payloads, as demonstrated by a single admin/reports/reportSchemaXml.form request.

- MISC - https://isears.github.io/jekyll/update/2017/10/21/openmrs-rce.html
- MISC - https://talk.openmrs.org/t/critical-security-advisory-2017-09-12/13291
- MISC - https://wiki.openmrs.org/display/RES/Release+Notes+2.6.1

Vulnerable Software & Versions:

- cpe:/a:openmrs:openmrs:2.1::~~standalone~~~

serialization.xstream-api-0.2.14.jar

Description:

API project for Serialization Xstream

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\serialization.xstream\lib\serialization.xstream-api-0.2.14.jar
MD5: 30e619f72568656fcdc85952ad61054f
SHA1: 76d70c10c7a39157ae30bfc2b18c5c7010c99fd3
SHA256:67f46c5f4e76fc63381cc660d91ad53342305199e8acf937f2964e87aecf989a

Evidence

Related Dependencies

Identifiers

- **maven:** org.openmrs.module:serialization.xstream-api:0.2.14 *Confidence*:High
- **cpe:** cpe:/a:xstream_project:xstream:0.2.14 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2016-3674 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-200 Information Exposure

Multiple XML external entity (XXE) vulnerabilities in the (1) Dom4JDriver, (2) DomDriver, (3) JDomDriver, (4) JDom2Driver, (5) SjsxpDriver, (6) StandardStaxDriver, and (7) WstxDriver drivers in XStream before 1.4.9 allow remote attackers to read arbitrary files via a crafted XML document.

- BID - 85381
- CONFIRM - http://x-stream.github.io/changes.html#1.4.9
- CONFIRM - https://github.com/x-stream/xstream/issues/25
- DEBIAN - DSA-3575
- FEDORA - FEDORA-2016-250042b8a6
- FEDORA - FEDORA-2016-de909cc333
- MLIST - [oss-security] 20160325 CVE request - XStream: XXE vulnerability
- MLIST - [oss-security] 20160328 Re: CVE request - XStream: XXE vulnerability
- REDHAT - RHSA-2016:2822
- REDHAT - RHSA-2016:2823
- SECTRACK - 1036419

Vulnerable Software & Versions:

- cpe:/a:xstream_project:xstream:1.4.8 and all previous versions

CVE-2017-7957 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-20 Improper Input Validation

XStream through 1.4.9, when a certain denyTypes workaround is not used, mishandles attempts to create an instance of the primitive type 'void' during unmarshalling, leading to a remote application crash, as demonstrated by an xstream.fromXML("<void/>") call.

- BID - 100687
- CONFIRM - http://x-stream.github.io/CVE-2017-7957.html
- CONFIRM - https://www-prd-trops.events.ibm.com/node/715749
- DEBIAN - DSA-3841
- REDHAT - RHSA-2017:1832
- REDHAT - RHSA-2017:2888
- REDHAT - RHSA-2017:2889
- SECTRACK - 1039499
- XF - xstream-cve20177957-dos(125800)

Vulnerable Software & Versions:

- cpe:/a:xstream_project:xstream:1.4.9 and all previous versions

ognl-3.0.8.jar

Description:

OGNL - Object Graph Navigation Library

License:

The Apache Software License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\fhir\lib\ognl-3.0.8.jar
MD5: 6f2969f0eb541a6f4ecfa15faa8155d7
SHA1: 37e1aebfde7eb7baebc9ad4f85116ef9009c5fc5
SHA256:97c13090ba9f1b2c34a9548461423e734252dafe0774af55c53d248c736e488c

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:ognl_project:ognl:3.0.8 *Confidence*:Low suppress
- **maven:** ognl:ognl:3.0.8 *Confidence*:High

Published Vulnerabilities

CVE-2016-3093 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-20 Improper Input Validation

Apache Struts 2.0.0 through 2.3.24.1 does not properly cache method references when used with OGNL before 3.0.12, which allows remote attackers to cause a denial of service (block access to a web site) via unspecified vectors.

- BID - 90961
- CONFIRM - http://struts.apache.org/docs/s2-034.html
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21987854
- SECTRACK - 1036018

Vulnerable Software & Versions: (show all)

- cpe:/a:ognl_project:ognl:3.0.11 and all previous versions
- ...

solr-core-4.10.4.jar

Description:

Apache Solr Core

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\chartsearch\lib\solr-core-4.10.4.jar
MD5: 06d09ccfcc16895ddac18fb6716e9fc6
SHA1: 4c5c49c4c8512ec96075a73534b63a18e9184eba
SHA256:edc52a7c77e21e94fe11e6fefd5baa8173d377d5912db7f50ea88a9b5d93e474

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:apache:solr:4.10.4 *Confidence*:Low suppress
- **maven:** org.apache.solr:solr-core:4.10.4 ✓ *Confidence*:Highest

Published Vulnerabilities

CVE-2015-8795 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Multiple cross-site scripting (XSS) vulnerabilities in the Admin UI in Apache Solr before 5.1 allow remote attackers to inject arbitrary web script or HTML via crafted fields that are mishandled during the rendering of the (1) Analysis page, related to webapp/web/js/scripts/analysis.js or (2) Schema-Browser page, related to webapp/web/js/scripts/schema-browser.js.

- CONFIRM - https://issues.apache.org/jira/browse/SOLR-7346

Vulnerable Software & Versions:

- cpe:/a:apache:solr:5.0 and all previous versions

CVE-2015-8796 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in webapp/web/js/scripts/schema-browser.js in the Admin UI in Apache Solr before 5.3 allows remote attackers to inject arbitrary web script or HTML via a crafted schema-browse URL.

- BID - 85205
- CONFIRM - https://issues.apache.org/jira/browse/SOLR-7920

Vulnerable Software & Versions:

- cpe:/a:apache:solr:5.2.1 and all previous versions

CVE-2015-8797 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in webapp/web/js/scripts/plugins.js in the stats page in the Admin UI in Apache Solr before 5.3.1 allows remote attackers to inject arbitrary web script or HTML via the entry parameter to a plugins/cache URI.

- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21975544
- CONFIRM - https://issues.apache.org/jira/browse/SOLR-7949

Vulnerable Software & Versions:

- cpe:/a:apache:solr:5.3 and all previous versions

CVE-2017-3163 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

When using the Index Replication feature, Apache Solr nodes can pull index files from a master/leader node using an HTTP API which accepts a file name. However, Solr before 5.5.4 and 6.x before 6.4.1 did not validate the file name, hence it was possible to craft a special request involving path traversal, leaving any file readable to the Solr server process exposed. Solr servers protected and restricted by firewall rules and/or authentication would not be at risk since only trusted clients and users would gain direct HTTP access.

- DEBIAN - DSA-4124
- MLIST - [solr-user] 20170215 [SECURITY] CVE-2017-3163 Apache Solr ReplicationHandler path traversal attack
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:solr:5.5.3 and all previous versions
- ...

mysql.exe

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\database\bin\mysql.exe
MD5: 53a286ae7ae55aa4c1db30fcf48bcfbd
SHA1: 3748c09d66b6e6d27f4c006e95e9f3863eeeaba6
SHA256:a798316910f1bce3291553210d2e0ca6a67d6a9f023a1580fd4bac60b4030de0

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:mysql:mysql:- *Confidence*:Low suppress

Published Vulnerabilities

CVE-2001-0407 suppress

Severity:Medium
CVSS Score: 4.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

Directory traversal vulnerability in MySQL before 3.23.36 allows local users to modify arbitrary files and gain privileges by creating a database whose name starts with .. (dot dot).

- BID - 2522
- BUGTRAQ - 20010318 potential vulnerability of mysqld running with root privileges (can be used as good DoS or r00t expoloit)
- BUGTRAQ - 20010327 MySQL 3.23.36 is relased (fwd)
- XF - mysql-dot-directory-traversal(6617)

Vulnerable Software & Versions:

- cpe:/a:mysql:mysql:3.23.36 and all previous versions

CVE-2001-1274 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Buffer overflow in MySQL before 3.23.31 allows attackers to cause a denial of service and possibly gain privileges.

- CALDERA - CSSA-2001-006.0
- CONECTIVA - CLA-2001:375
- CONFIRM - http://www.mysql.com/documentation/mysql/bychapter/manual_News.html#News-3.23.3
- DEBIAN - DSA-013
- FREEBSD - FreeBSD-SA-01:16
- MANDRAKE - MDKSA-2001:014
- REDHAT - RHSA-2001:003

Vulnerable Software & Versions:

- cpe:/a:mysql:mysql:3.23.31 and all previous versions

CVE-2001-1275 suppress

Severity:High
CVSS Score: 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

MySQL before 3.23.31 allows users with a MySQL account to use the SHOW GRANTS command to obtain the encrypted administrator password from the mysql.user table and possibly gain privileges via password cracking.

- CALDERA - CSSA-2001-006.0
- FREEBSD - FreeBSD-SA-01:16
- MANDRAKE - MDKSA-2001:014
- REDHAT - RHSA-2001:003

Vulnerable Software & Versions:

- cpe:/a:mysql:mysql:3.23.31 and all previous versions

CVE-2001-1454 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Buffer overflow in MySQL before 3.23.33 allows remote attackers to execute arbitrary code via a long drop database request.

- BUGTRAQ - 20010209 Some more MySql security issues
- CERT-VN - VU#367320
- CONFIRM - http://dev.mysql.com/doc/mysql/en/news-3-23-33.html
- XF - mysql-drop-database-bo(6419)

Vulnerable Software & Versions:

- cpe:/a:mysql:mysql:3.23.32 and all previous versions

CVE-2003-1331 suppress

Severity:Medium
CVSS Score: 4.0 (AV:N/AC:H/Au:N/C:N/I:P/A:P)

Stack-based buffer overflow in the mysql_real_connect function in the MySql client library (libmysqlclient) 4.0.13 and earlier allows local users to execute arbitrary code via a long socket name, a different vulnerability than CVE-2001-1453.

- BID - 7887
- CONFIRM - http://bugs.mysql.com/bug.php?id=564
- FULLDISC - 20030612 libmysqlclient 4.x and below mysql_real_connect() buffer overflow.
- XF - mysql-mysqlrealconnect-bo(12337)

Vulnerable Software & Versions:

- cpe:/a:mysql:mysql:4.0.9:gamma and all previous versions

CVE-2004-0457 suppress

Severity:Medium
CVSS Score: 4.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

The mysqlhotcopy script in mysql 4.0.20 and earlier, when using the scp method from the mysql-server package, allows local users to overwrite arbitrary files via a symlink attack on temporary files.

- CIAC - P-018
- DEBIAN - DSA-540
- REDHAT - RHSA-2004:597
- XF - mysql-mysqlhotcopy-insecure-file(17030)

Vulnerable Software & Versions:

- cpe:/a:mysql:mysql:4.0.20 and all previous versions

CVE-2004-0835 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

MySQL 3.x before 3.23.59, 4.x before 4.0.19, 4.1.x before 4.1.2, and 5.x before 5.0.1, checks the CREATE/INSERT rights of the original table instead of the target table in an ALTER TABLE RENAME operation, which could allow attackers to conduct unauthorized activities.

- BID - 11357
- CIAC - P-018
- CONECTIVA - CLA-2004:892
- CONFIRM - http://www.mysql.org/doc/refman/4.1/en/news-4-0-19.html
- CONFIRM - http://www.mysql.org/doc/refman/4.1/en/news-4-1-2.html
- DEBIAN - DSA-562
- GENTOO - GLSA-200410-22
- MISC - http://bugs.mysql.com/bug.php?id=3270
- MISC - http://lists.mysql.com/internals/13073
- REDHAT - RHSA-2004:597
- REDHAT - RHSA-2004:611
- SECTRACK - 1011606
- SUNALERT - 101864
- TRUSTIX - 2004-0054
- XF - mysql-alter-restriction-bypass(17666)

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:3.23.59 and all previous versions
- ...

CVE-2004-0836 suppress

Severity:High
CVSS Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
CWE: CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

Buffer overflow in the mysql_real_connect function in MySQL 4.x before 4.0.21, and 3.x before 3.23.49, allows remote DNS servers to cause a denial of service and possibly execute arbitrary code via a DNS response with a large address length (h_length).

- BID - 10981
- BUGTRAQ - 20041125 [USN-32-1] mysql vulnerabilities
- CIAC - P-018
- CONECTIVA - CLA-2004:892
- DEBIAN - DSA-562
- GENTOO - GLSA-200410-22
- MISC - http://bugs.mysql.com/bug.php?id=4017
- MISC - http://lists.mysql.com/internals/14726
- REDHAT - RHSA-2004:597
- REDHAT - RHSA-2004:611
- TRUSTIX - 2004-0054
- XF - mysql-realconnect-bo(17047)

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:3.23.49 and all previous versions
- ...

CVE-2004-0837 suppress

Severity:Low
CVSS Score: 2.6 (AV:N/AC:H/Au:N/C:N/I:N/A:P)

MySQL 4.x before 4.0.21, and 3.x before 3.23.49, allows attackers to cause a denial of service (crash or hang) via multiple threads that simultaneously alter MERGE table UNIONs.

- BID - 11357
- BUGTRAQ - 20041125 [USN-32-1] mysql vulnerabilities
- CIAC - P-018
- CONECTIVA - CLA-2004:892
- DEBIAN - DSA-562
- GENTOO - GLSA-200410-22
- MISC - http://bugs.mysql.com/2408
- MISC - http://lists.mysql.com/internals/16168
- MISC - http://lists.mysql.com/internals/16173
- MISC - http://lists.mysql.com/internals/16174
- MISC - http://mysql.bkbits.net:8080/mysql-3.23/diffs/myisammrg/myrg_open.c@1.15
- REDHAT - RHSA-2004:597
- REDHAT - RHSA-2004:611
- SECTRACK - 1011606
- SUNALERT - 101864
- TRUSTIX - 2004-0054
- XF - mysql-union-dos(17667)

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:3.23.49 and all previous versions
- ...

CVE-2006-7232 suppress

Severity:Low
CVSS Score: 3.5 (AV:N/AC:M/Au:S/C:N/I:N/A:P)
CWE: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

sql_select.cc in MySQL 5.0.x before 5.0.32 and 5.1.x before 5.1.14 allows remote authenticated users to cause a denial of service (crash) via an EXPLAIN SELECT FROM on the INFORMATION_SCHEMA table, as originally demonstrated using ORDER BY.

- BID - 28351
- CONFIRM - http://bugs.mysql.com/bug.php?id=22413
- CONFIRM - http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-32.html
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-14.html
- REDHAT - RHSA-2008:0364
- SUSE - SUSE-SR:2008:017
- UBUNTU - USN-588-1

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:5.1.13 and all previous versions
- ...

CVE-2007-1420 suppress

Severity:Low
CVSS Score: 2.1 (AV:L/AC:L/Au:N/C:N/I:N/A:P)

MySQL 5.x before 5.0.36 allows local users to cause a denial of service (database crash) by performing information_schema table subselects and using ORDER BY to sort a single-row result, which prevents certain structure elements from being initialized and triggers a NULL dereference in the filesort function.

- BID - 22900
- BUGTRAQ - 20070309 SEC Consult SA-20070309-0 :: MySQL 5 Single Row Subselect Denial of Service
- CONFIRM - http://bugs.mysql.com/bug.php?id=24630
- CONFIRM - http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-36.html
- CONFIRM - https://issues.rpath.com/browse/RPL-1127
- GENTOO - GLSA-200705-11
- MANDRIVA - MDKSA-2007:139
- MISC - http://www.sec-consult.com/284.html
- REDHAT - RHSA-2008:0364
- SECTRACK - 1017746
- SREASON - 2413
- UBUNTU - USN-440-1
- VUPEN - ADV-2007-0908

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:5.0.33 and all previous versions
- ...

CVE-2007-2583 suppress

Severity:Medium
CVSS Score: 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)
CWE: CWE-189 Numeric Errors

The in_decimal::set function in item_cmpfunc.cc in MySQL before 5.0.40, and 5.1 before 5.1.18-beta, allows context-dependent attackers to cause a denial of service (crash) via a crafted IF clause that results in a divide-by-zero error and a NULL pointer dereference.

- BID - 23911
- CONFIRM - http://bugs.mysql.com/bug.php?id=27513
- CONFIRM - http://lists.mysql.com/commits/23685
- CONFIRM - https://issues.rpath.com/browse/RPL-1356
- DEBIAN - DSA-1413
- EXPLOIT-DB - 30020
- GENTOO - GLSA-200705-11
- MANDRIVA - MDKSA-2007:139
- MISC - http://packetstormsecurity.com/files/124295/MySQL-5.0.x-Denial-Of-Service.html
- REDHAT - RHSA-2008:0364
- SUSE - SUSE-SR:2008:003
- TRUSTIX - 2007-0017
- UBUNTU - USN-528-1
- VUPEN - ADV-2007-1731
- XF - mysql-if-dos(34232)

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:5.0.38 and all previous versions
- ...

CVE-2007-2691 suppress

Severity:Medium
CVSS Score: 4.9 (AV:N/AC:M/Au:S/C:N/I:P/A:P)

MySQL before 4.1.23, 5.0.x before 5.0.42, and 5.1.x before 5.1.18 does not require the DROP privilege for RENAME TABLE statements, which allows remote authenticated users to rename arbitrary tables.

- APPLE - APPLE-SA-2008-10-09
- BID - 24016
- BID - 31681
- BUGTRAQ - 20070717 rPSA-2007-0143-1 mysql mysql-bench mysql-server
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-18.html
- CONFIRM - http://support.apple.com/kb/HT3216
- CONFIRM - https://issues.rpath.com/browse/RPL-1536
- DEBIAN - DSA-1413

- MANDRIVA - MDKSA-2007:139
- MISC - http://bugs.mysql.com/bug.php?id=27515
- MLIST - [announce] 20070712 MySQL Community Server 5.0.45 has been released!
- REDHAT - RHSA-2007:0894
- REDHAT - RHSA-2008:0364
- REDHAT - RHSA-2008:0768
- SECTRACK - 1018069
- SUSE - SUSE-SR:2008:003
- UBUNTU - USN-528-1
- VUPEN - ADV-2007-1804
- VUPEN - ADV-2008-2780
- XF - mysql-renametable-weak-security(34347)

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:5.0.41 and all previous versions
- ...

CVE-2007-5925 suppress

Severity:Medium
CVSS Score: 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)
CWE: CWE-20 Improper Input Validation

The convert_search_mode_to_innobase function in ha_innodb.cc in the InnoDB engine in MySQL 5.1.23-BK and earlier allows remote authenticated users to cause a denial of service (database crash) via a certain CONTAINS operation on an indexed column, which triggers an assertion error.

- BID - 26353
- CONFIRM - http://bugs.gentoo.org/show_bug.cgi?id=198988
- CONFIRM - http://bugs.mysql.com/bug.php?id=32125
- DEBIAN - DSA-1413
- FEDORA - FEDORA-2007-4465
- FEDORA - FEDORA-2007-4471
- FULLDISC - 20071106 MySQL 5.x DoS (unknown)
- GENTOO - GLSA-200711-25
- MANDRIVA - MDKSA-2007:243
- REDHAT - RHSA-2007:1155
- REDHAT - RHSA-2007:1157
- SECTRACK - 1018978
- SLACKWARE - SSA:2007-348-01
- SUSE - SUSE-SR:2008:003
- UBUNTU - USN-1397-1
- UBUNTU - USN-559-1
- VUPEN - ADV-2007-3903
- XF - mysql-hainnodb-dos(38284)

Vulnerable Software & Versions:

- cpe:/a:mysql:mysql:5.1.23_bk and all previous versions

CVE-2008-2079 suppress

Severity:Medium
CVSS Score: 4.6 (AV:N/AC:H/Au:S/C:P/I:P/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

MySQL 4.1.x before 4.1.24, 5.0.x before 5.0.60, 5.1.x before 5.1.24, and 6.0.x before 6.0.5 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are within the MySQL home data directory, which can point to tables that are created in the future.

- APPLE - APPLE-SA-2008-10-09
- APPLE - APPLE-SA-2009-09-10-2
- BID - 29106
- BID - 31681
- CONFIRM - http://bugs.mysql.com/bug.php?id=32167
- CONFIRM - http://dev.mysql.com/doc/refman/4.1/en/news-4-1-24.html
- CONFIRM - http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-60.html
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-24.html
- CONFIRM - http://dev.mysql.com/doc/refman/6.0/en/news-6-0-5.html
- CONFIRM - http://support.apple.com/kb/HT3216
- CONFIRM - http://support.apple.com/kb/HT3865
- DEBIAN - DSA-1608
- MANDRIVA - MDVSA-2008:149
- MANDRIVA - MDVSA-2008:150
- REDHAT - RHSA-2008:0505
- REDHAT - RHSA-2008:0510
- REDHAT - RHSA-2008:0768
- REDHAT - RHSA-2009:1289
- SECTRACK - 1019995
- SUSE - SUSE-SR:2008:017
- UBUNTU - USN-671-1
- VUPEN - ADV-2008-1472
- VUPEN - ADV-2008-2780
- XF - mysql-myisam-security-bypass(42267)

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:6.0.4 and all previous versions
- ...

CVE-2009-0819 suppress

Severity:Medium
CVSS Score: 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)

sql/item_xmlfunc.cc in MySQL 5.1 before 5.1.32 and 6.0 before 6.0.10 allows remote authenticated users to cause a denial of service (crash) via "an XPath expression employing a scalar expression as a FilterExpr with ExtractValue() or UpdateXML()," which triggers an assertion failure.

- BID - 33972
- CONFIRM - http://bugs.mysql.com/bug.php?id=42495
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-32.html
- CONFIRM - http://dev.mysql.com/doc/refman/6.0/en/news-6-0-10.html
- SECTRACK - 1021786
- VUPEN - ADV-2009-0594
- XF - mysql-xpath-dos(49050)

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:5.1.32-bzr and all previous versions
- ...

CVE-2009-4028 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-20 Improper Input Validation

The vio_verify_callback function in viosslfactories.c in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41, when OpenSSL is used, accepts a value of zero for the depth of X.509 certificates, which allows man-in-the-middle attackers to spoof arbitrary SSL-based MySQL servers via a crafted certificate, as demonstrated by a certificate presented by a server linked against the yaSSL library.

- CONFIRM - http://bugs.mysql.com/47320
- CONFIRM - http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html
- MLIST - [commits] 20091020 bzr commit into mysql-4.1 branch (joro:2709) Bug#47320
- MLIST - [oss-security] 20091119 mysql-5.1.41
- MLIST - [oss-security] 20091121 CVE Request - MySQL - 5.0.88
- MLIST - [oss-security] 20091123 Re: mysql-5.1.41
- REDHAT - RHSA-2010:0109
- SUSE - SUSE-SR:2010:011
- VUPEN - ADV-2010-1107

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:5.0.87 and all previous versions
- ...

CVE-2010-1621 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-264 Permissions, Privileges, and Access Controls

The mysql_uninstall_plugin function in sql/sql_plugin.cc in MySQL 5.1 before 5.1.46 does not check privileges before uninstalling a plugin, which allows remote attackers to uninstall arbitrary plugins via the UNINSTALL PLUGIN command.

- BID - 39543
- CONFIRM - http://bugs.mysql.com/bug.php?id=51770
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-46.html
- MANDRIVA - MDVSA-2010:093
- UBUNTU - USN-1397-1

Vulnerable Software & Versions:

- cpe:/a:mysql:mysql:5.1.45 and all previous versions

CVE-2010-1626 suppress

Severity:Low
CVSS Score: 3.6 (AV:L/AC:L/Au:N/C:N/I:P/A:P)
CWE: CWE-59 Improper Link Resolution Before File Access ('Link Following')

MySQL before 5.1.46 allows local users to delete the data and index files of another user's MyISAM table via a symlink attack in conjunction with the DROP TABLE command, a different vulnerability than CVE-2008-4098 and CVE-2008-7247.

- BID - 40257
- CONFIRM - http://bugs.mysql.com/bug.php?id=40980
- MANDRIVA - MDVSA-2010:101
- MLIST - [oss-security] 20100510 Re: A mysql flaw.
- MLIST - [oss-security] 20100518 Re: A mysql flaw.
- REDHAT - RHSA-2010:0442
- SECTRACK - 1024004
- SUSE - SUSE-SR:2010:019
- SUSE - SUSE-SR:2010:021
- UBUNTU - USN-1397-1
- VUPEN - ADV-2010-1194

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:5.1.45 and all previous versions
- ...

CVE-2010-2008 suppress

Severity:Low
CVSS Score: 3.5 (AV:N/AC:M/Au:S/C:N/I:N/A:P)
CWE: CWE-20 Improper Input Validation

MySQL before 5.1.48 allows remote authenticated users with alter database privileges to cause a denial of service (server crash and database loss) via an ALTER DATABASE command with a #mysql50# string followed by a . (dot), .. (dot dot), ../ (dot dot slash) or similar sequence, and an UPGRADE DATA DIRECTORY NAME command, which causes MySQL to move certain directories to the server data directory.

- BID - 41198
- CONFIRM - http://bugs.mysql.com/bug.php?id=53804
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-48.html
- FEDORA - FEDORA-2010-11135

- MANDRIVA - MDVSA-2010:155
- SECTRACK - 1024160
- UBUNTU - USN-1017-1
- UBUNTU - USN-1397-1
- VUPEN - ADV-2010-1918

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:5.1.47 and all previous versions
- ...

CVE-2010-3677 suppress

Severity:Medium
CVSS Score: 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)
CWE: CWE-399 Resource Management Errors

Oracle MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated users to cause a denial of service (mysqld daemon crash) via a join query that uses a table with a unique SET column.

- APPLE - APPLE-SA-2011-06-23-1
- BID - 42646
- CONFIRM - http://dev.mysql.com/doc/refman/5.0/en/news-5-0-92.html
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html
- CONFIRM - http://support.apple.com/kb/HT4723
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=628040
- DEBIAN - DSA-2143
- MANDRIVA - MDVSA-2010:155
- MANDRIVA - MDVSA-2010:222
- MANDRIVA - MDVSA-2011:012
- MISC - http://bugs.mysql.com/bug.php?id=54575
- MLIST - [oss-security] 20100928 Re: CVE Request -- MySQL v5.1.49 -- multiple DoS flaws
- REDHAT - RHSA-2010:0825
- REDHAT - RHSA-2011:0164
- SUSE - SUSE-SR:2010:019
- TURBO - TLSA-2011-3
- UBUNTU - USN-1017-1
- UBUNTU - USN-1397-1
- VUPEN - ADV-2011-0105
- VUPEN - ADV-2011-0133
- VUPEN - ADV-2011-0170
- VUPEN - ADV-2011-0345
- XF - mysql-setcolumn-dos(64688)

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:5.0.91 and all previous versions
- ...

CVE-2010-3682 suppress

Severity:Medium
CVSS Score: 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)

Oracle MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated users to cause a denial of service (mysqld daemon crash) by using EXPLAIN with crafted "SELECT ... UNION ... ORDER BY (SELECT ... WHERE ...)" statements, which triggers a NULL pointer dereference in the Item_singlerow_subselect::store function.

- APPLE - APPLE-SA-2011-06-23-1
- BID - 42599
- CONFIRM - http://bugs.mysql.com/bug.php?id=52711
- CONFIRM - http://dev.mysql.com/doc/refman/5.0/en/news-5-0-92.html
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html
- CONFIRM - http://support.apple.com/kb/HT4723
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=628328
- DEBIAN - DSA-2143
- MANDRIVA - MDVSA-2010:155
- MANDRIVA - MDVSA-2010:222
- MANDRIVA - MDVSA-2011:012
- MLIST - [oss-security] 20100928 Re: CVE Request -- MySQL v5.1.49 -- multiple DoS flaws
- REDHAT - RHSA-2010:0825
- REDHAT - RHSA-2011:0164
- SUSE - SUSE-SR:2010:019
- TURBO - TLSA-2011-3
- UBUNTU - USN-1017-1
- UBUNTU - USN-1397-1
- VUPEN - ADV-2011-0105
- VUPEN - ADV-2011-0133
- VUPEN - ADV-2011-0170
- VUPEN - ADV-2011-0345
- XF - mysql-itemsinglerowsubselect-dos(64684)

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:5.0.91 and all previous versions
- ...

CVE-2012-5627 suppress

Severity:Medium
CVSS Score: 4.0 (AV:N/AC:L/Au:S/C:P/I:N/A:N)
CWE: CWE-255 Credentials Management

Oracle MySQL and MariaDB 5.5.x before 5.5.29, 5.3.x before 5.3.12, and 5.2.x before 5.2.14 does not modify the salt during multiple executions of the change_user command within the same connection which makes it easier for remote authenticated users to conduct brute force password guessing attacks.

- CONFIRM - https://mariadb.atlassian.net/browse/MDEV-3915
- FULLDISC - 20121203 MySQL Local/Remote FAST Account Password Cracking

- FULLDISC - 20121205 Re: MySQL Local/Remote FAST Account Password Cracking
- GENTOO - GLSA-201308-06
- MANDRIVA - MDVSA-2013:102
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=883719
- MLIST - [oss-security] 20121206 Re: CVE request: Mysql/Mariadb insecure salt-usage

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql
- ...

CVE-2013-0375 suppress

Severity:Medium
CVSS Score: 5.5 (AV:N/AC:L/Au:S/C:P/I:P/A:N)
CWE: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.1.28 and earlier, allows remote authenticated users to affect confidentiality and integrity via unknown vectors related to Server Replication.

- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpujan2013-1515902.html
- GENTOO - GLSA-201308-06
- MANDRIVA - MDVSA-2013:150
- REDHAT - RHSA-2013:0219
- UBUNTU - USN-1703-1

Vulnerable Software & Versions: (show all)

- cpe:/a:mysql:mysql:5.1.28 and all previous versions
- ...

CVE-2015-2575 suppress

Severity:Medium
CVSS Score: 4.9 (AV:N/AC:M/Au:S/C:P/I:P/A:N)

Unspecified vulnerability in the MySQL Connectors component in Oracle MySQL 5.1.34 and earlier allows remote authenticated users to affect confidentiality and integrity via unknown vectors related to Connector/J.

- BID - 74075
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
- CONFIRM - https://security.netapp.com/advisory/ntap-20150417-0003/
- DEBIAN - DSA-3621
- SECTRACK - 1032121
- SUSE - SUSE-SU-2015:0946
- SUSE - openSUSE-SU-2015:0967

Vulnerable Software & Versions:

- cpe:/a:mysql:mysql:5.1.34 and all previous versions

dwr-2.0.7-mod.jar

Description:

DWR is easy Ajax for Java. It makes it simple to call Java code directly from Javascript.
It gets rid of almost all the boiler plate code between the web browser and your Java code.
Customized for OpenMRS (see README in META-INF)

License:

The Apache Software License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\legacyui\lib\dwr-2.0.7-mod.jar
MD5: 1ad810c01f9be26c959069e93577e6fa
SHA1: db0daaaa2202de70df020c1d3043776f48fcdadf
SHA256:c08a1ce7e0871df82f44243804b0e551d8dbb71b72e2326f5abb331b491143ec

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:directwebremoting:direct_web_remoting:2.0.7 *Confidence*:Low suppress
- **cpe:** cpe:/a:getahead:direct_web_remoting:2.0.7 *Confidence*:Low suppress
- **cpe:** cpe:/a:openmrs:openmrs:2.0.7 *Confidence*:Low suppress
- **maven:** org.openmrs.directwebremoting:dwr:2.0.5-mod *Confidence*:High

Published Vulnerabilities

CVE-2014-5325 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-200 Information Exposure

The (1) DOMConverter, (2) JDOMConverter, (3) DOM4JConverter, and (4) XOMConverter functions in Direct Web Remoting (DWR) through 2.0.10 and 3.x through 3.0.RC2 allow remote attackers to read arbitrary files via DOM data containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.

- BID - 71093
- JVN - JVN#91502163
- JVNDB - JVNDB-2014-000117

Vulnerable Software & Versions: (show all)

- cpe:/a:directwebremoting:direct_web_remoting:2.0.10 and all previous versions
- ...

CVE-2014-5326 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in Direct Web Remoting (DWR) through 2.0.10 and 3.x through 3.0.RC2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- JVN - JVN#52422792
- JVNDB - JVNDB-2014-000118

Vulnerable Software & Versions: (show all)

- cpe:/a:directwebremoting:direct_web_remoting:2.0.10 and all previous versions
- ...

activeio-core-3.1.2.jar

Description:

A high performance IO abstraction framework

License:

http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\event\lib\activeio-core-3.1.2.jar
MD5: 3e0593aba1d98a5bcaf18eb626f7838d
SHA1: 91348a918fcea7d967ca3f1bb8ed19065bbf819d
SHA256:e339fcf634354c14cab89fd735c79d10db14e577fc94a6ee37a8c38b588dbc51

Evidence

Related Dependencies

Identifiers

- **maven:** org.apache.activemq:activeio-core:3.1.2 *Confidence*:High
- **cpe:** cpe:/a:apache:activemq:3.1.2 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2010-0684 suppress

Severity:Low
CVSS Score: 3.5 (AV:N/AC:M/Au:S/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in createDestination.action in Apache ActiveMQ before 5.3.1 allows remote authenticated users to inject arbitrary web script or HTML via the JMSDestination parameter in a queue action.

- BID - 39119
- BUGTRAQ - 20100330 CVE-2010-0684: Apache ActiveMQ Persistent Cross-Site Scripting (XSS) Vulnerability
- CONFIRM - http://activemq.apache.org/activemq-531-release.html
- CONFIRM - https://issues.apache.org/activemq/browse/AMQ-2613
- CONFIRM - https://issues.apache.org/activemq/browse/AMQ-2625
- MISC - http://www.rajatswarup.com/CVE-2010-0684.txt
- SECTRACK - 1023778
- XF - activemq-createdestination-xss(57397)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.3.0 and all previous versions
- ...

CVE-2010-1244 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-352 Cross-Site Request Forgery (CSRF)

Cross-site request forgery (CSRF) vulnerability in createDestination.action in Apache ActiveMQ before 5.3.1 allows remote attackers to hijack the authentication of unspecified victims for requests that create queues via the JMSDestination parameter in a queue action.

- CONFIRM - http://activemq.apache.org/activemq-531-release.html
- CONFIRM - https://issues.apache.org/activemq/browse/AMQ-2613
- CONFIRM - https://issues.apache.org/activemq/browse/AMQ-2625
- XF - activemq-web-console-csrf(57398)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.3.0 and all previous versions
- ...

CVE-2011-4905 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-399 Resource Management Errors

Apache ActiveMQ before 5.6.0 allows remote attackers to cause a denial of service (file-descriptor exhaustion and broker crash or hang) by sending many openwire failover:tcp:// connection requests.

- BID - 50904
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1209700
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1211844
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-3294
- MLIST - [oss-security] 20111224 CVE Request for Apache ActiveMQ DoS
- MLIST - [oss-security] 20111225 Re: CVE Request for Apache ActiveMQ DoS

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.5.1 and all previous versions
- ...

CVE-2012-5784 suppress

Severity:Medium
CVSS Score: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)
CWE: CWE-20 Improper Input Validation

Apache Axis 1.4 and earlier, as used in PayPal Payments Pro, PayPal Mass Pay, PayPal Transactional Information SOAP, the Java Message Service implementation in Apache ActiveMQ, and other products, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- BID - 56408
- MISC - http://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf
- REDHAT - RHSA-2013:0269
- REDHAT - RHSA-2013:0683
- REDHAT - RHSA-2014:0037
- XF - apache-axis-ssl-spoofing(79829)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2012-6092 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Multiple cross-site scripting (XSS) vulnerabilities in the web demos in Apache ActiveMQ before 5.8.0 allow remote attackers to inject arbitrary web script or HTML via (1) the refresh parameter to PortfolioPublishServlet.java (aka demo/portfolioPublish or Market Data Publisher), or vectors involving (2) debug logs or (3) subscribe messages in webapp/websocket/chat.js. NOTE: AMQ-4124 is covered by CVE-2012-6551.

- BID - 59400
- CONFIRM - http://activemq.apache.org/activemq-580-release.html
- CONFIRM - https://fisheye6.atlassian.com/changelog/activemq?cs=1399577
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4115
- CONFIRM - https://issues.apache.org/jira/secure/ReleaseNote.jspa?projectId=12311210&version=12323282
- REDHAT - RHSA-2013:1029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2012-6551 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-399 Resource Management Errors

The default configuration of Apache ActiveMQ before 5.8.0 enables a sample web application, which allows remote attackers to cause a denial of service (broker resource consumption) via HTTP requests.

- BID - 59401
- CONFIRM - http://activemq.apache.org/activemq-580-release.html
- CONFIRM - https://fisheye6.atlassian.com/changelog/activemq?cs=1404998

- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4124
- CONFIRM - https://issues.apache.org/jira/secure/ReleaseNote.jspa?projectId=12311210&version=12323282
- MLIST - [dev] 20121022 [DISCUSS] - ActiveMQ out of the box - Should not include the demos
- REDHAT - RHSA-2013:1029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2013-1879 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in scheduled.jsp in Apache ActiveMQ 5.8.0 and earlier allows remote attackers to inject arbitrary web script or HTML via vectors involving the "cron of a message."

- BID - 61142
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4397
- REDHAT - RHSA-2013:1029
- XF - activemq-cve20131879-xss(85586)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.8.0 and all previous versions
- ...

CVE-2013-1880 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in the Portfolio publisher servlet in the demo web application in Apache ActiveMQ before 5.9.0 allows remote attackers to inject arbitrary web script or HTML via the refresh parameter to demo/portfolioPublish, a different vulnerability than CVE-2012-6092.

- BID - 65615
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=924447
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4398
- REDHAT - RHSA-2013:1029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.8.0 and all previous versions
- ...

CVE-2013-3060 suppress

Severity:Medium
CVSS Score: 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)
CWE: CWE-287 Improper Authentication

The web console in Apache ActiveMQ before 5.8.0 does not require authentication, which allows remote attackers to obtain sensitive information or cause a denial of service via HTTP requests.

- BID - 59402
- CONFIRM - http://activemq.apache.org/activemq-580-release.html
- CONFIRM - https://fisheye6.atlassian.com/changelog/activemq?cs=1404998
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4124
- CONFIRM - https://issues.apache.org/jira/secure/ReleaseNote.jspa?projectId=12311210&version=12323282
- MLIST - [dev] 20121022 [DISCUSS] - ActiveMQ out of the box - Should not include the demos
- REDHAT - RHSA-2013:1029
- REDHAT - RHSA-2013:1221

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2014-3576 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

The processControlCommand function in broker/TransportConnection.java in Apache ActiveMQ before 5.11.0 allows remote attackers to cause a denial of service (shutdown) via a shutdown command.

- BID - 76272
- BUGTRAQ - 20151106 [ANNOUNCE] CVE-2014-3576 - Apache ActiveMQ vulnerabilities
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
- CONFIRM - https://github.com/apache/activemq/commit/00921f2
- DEBIAN - DSA-3330
- MISC - http://packetstormsecurity.com/files/134274/Apache-ActiveMQ-5.10.1-Denial-Of-Service.html
- MLIST - [dev] 20150721 About CVE-2014-3576
- SECTRACK - 1033898

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.10.0 and all previous versions
- ...

CVE-2015-5182 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CWE: CWE-352 Cross-Site Request Forgery (CSRF)

Cross-site request forgery (CSRF) vulnerability in the jolokia API in A-MQ.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1248809

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:-

CVE-2015-5183 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-254 7PK - Security Features

The Hawtio console in A-MQ does not set HTTPOnly or Secure attributes on cookies.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1249182

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:-

CVE-2015-5184 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-254 7PK - Security Features

The Hawtio console in A-MQ allows remote attackers to obtain sensitive information and perform other unspecified impact.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1249183

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:-

CVE-2016-3088 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-20 Improper Input Validation

The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.

- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2016-3088-announcement.txt
- EXPLOIT-DB - 42283
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-16-356
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-16-357
- REDHAT - RHSA-2016:2036
- SECTRACK - 1035951

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:5.13.3 and all previous versions

struts-core-1.3.8.jar

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\tomcat\webapps\openmrs-standalone\WEB-INF\lib\struts-core-1.3.8.jar
MD5: 868de456b4d4331d6dcc4e8d3bee884e
SHA1: 66178d4a9279ebb1cd1eb79c10dc204b4199f061
SHA256:a7881710517dd6a50fa81c04d494e1493ad326bcc1adf2eb9493e5eb9ca9e077

Evidence

Related Dependencies

Identifiers

- **maven:** org.apache.struts:struts-core:1.3.8 *Confidence*:High
- **cpe:** cpe:/a:apache:struts:1.3.8 *Confidence*:Highest suppress

Published Vulnerabilities

CVE-2014-0114 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-20 Improper Input Validation

Apache Commons BeanUtils, as distributed in lib/commons-beanutils-1.8.0.jar in Apache Struts 1.x through 1.3.10 and in other products requiring commons-beanutils through 1.9.2, does not suppress the class property, which allows remote attackers to "manipulate" the ClassLoader and execute arbitrary code via the class parameter, as demonstrated by the passing of this parameter to the getClass method of the ActionForm object in Struts 1.

- BID - 67121
- BUGTRAQ - 20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
- CONFIRM - http://advisories.mageia.org/MGASA-2014-0219.html
- CONFIRM - http://commons.apache.org/proper/commons-beanutils/javadocs/v1.9.2/RELEASE-NOTES.txt
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21674128
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21674812
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675266
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675387
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675689
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675898
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675972
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676091
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676110
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676303
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676375
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676931
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21677110
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg27042296
- CONFIRM - http://www.ibm.com/support/docview.wss?uid=swg21675496
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
- CONFIRM - http://www.vmware.com/security/advisories/VMSA-2014-0008.html
- CONFIRM - http://www.vmware.com/security/advisories/VMSA-2014-0012.html
- CONFIRM - https://access.redhat.com/solutions/869353
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1091938
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1116665
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05324755
- CONFIRM - https://issues.apache.org/jira/browse/BEANUTILS-463
- CONFIRM - https://security.netapp.com/advisory/ntap-20140911-0001/
- CONFIRM - https://security.netapp.com/advisory/ntap-20180629-0006/
- DEBIAN - DSA-2940
- FEDORA - FEDORA-2014-9380
- FULLDISC - 20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
- GENTOO - GLSA-201607-09
- HP - HPSBGN03041
- HP - HPSBMU03090
- HP - HPSBST03160
- MANDRIVA - MDVSA-2014:095
- MLIST - [apache-ignite-developers] 20180601 [CVE-2014-0114]: Apache Ignite is vulnerable to existing CVE-2014-0114
- MLIST - [oss-security] 20140616 CVE request for commons-beanutils: 'class' property is exposed, potentially leading to RCE
- MLIST - [oss-security] 20140707 Re: CVE request for commons-beanutils: 'class' property is exposed, potentially leading to RCE
- SECUNIA - 57477
- SECUNIA - 58710
- SECUNIA - 58947
- SECUNIA - 59118
- SECUNIA - 59228
- SECUNIA - 59245
- SECUNIA - 59246
- SECUNIA - 59430
- SECUNIA - 59464
- SECUNIA - 59479
- SECUNIA - 59480
- SECUNIA - 59718

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:struts:1.3.8
- ...

CVE-2015-0899 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-20 Improper Input Validation

The MultiPageValidator implementation in Apache Struts 1 1.1 through 1.3.10 allows remote attackers to bypass intended access restrictions via a modified page parameter.

- BID - 74423
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - https://en.osdn.jp/projects/terasoluna/wiki/StrutsPatch2-EN
- CONFIRM - https://security.netapp.com/advisory/ntap-20180629-0006/
- DEBIAN - DSA-3536
- JVN - JVN#86448949
- JVNDB - JVNDB-2015-000042

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:struts:1.3.8
- ...

CVE-2016-1181 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

ActionServlet.java in Apache Struts 1 1.x through 1.3.10 mishandles multithreaded access to an ActionForm instance, which allows remote attackers to execute arbitrary code or cause a denial of service (unexpected memory access) via a multipart request, a related issue to CVE-2015-0899.

- BID - 91068
- BID - 91787
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1343538
- CONFIRM - https://github.com/kawasima/struts1-forever/commit/eda3a79907ed8fcb0387a0496d0cb14332f250e8
- CONFIRM - https://security-tracker.debian.org/tracker/CVE-2016-1181
- CONFIRM - https://security.netapp.com/advisory/ntap-20180629-0006/
- JVN - JVN#03188560
- JVNDB - JVNDB-2016-000096
- SECTRACK - 1036056

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:struts:1.3.8
- ...

CVE-2016-1182 suppress

Severity:Medium
CVSS Score: 6.4 (AV:N/AC:L/Au:N/C:N/I:P/A:P)
CWE: CWE-20 Improper Input Validation

ActionServlet.java in Apache Struts 1 1.x through 1.3.10 does not properly restrict the Validator configuration, which allows remote attackers to conduct cross-site scripting (XSS) attacks or cause a denial of service via crafted input, a related issue to CVE-2015-0899.

- BID - 91067
- BID - 91787
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1343540
- CONFIRM - https://github.com/kawasima/struts1-forever/commit/eda3a79907ed8fcb0387a0496d0cb14332f250e8
- CONFIRM - https://security-tracker.debian.org/tracker/CVE-2016-1182
- CONFIRM - https://security.netapp.com/advisory/ntap-20180629-0006/
- JVN - JVN#65044642
- JVNDB - JVNDB-2016-000097
- SECTRACK - 1036056

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:struts:1.3.8
- ...

struts-tiles-1.3.8.jar

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\tomcat\webapps\openmrs-standalone\WEB-INF\lib\struts-tiles-1.3.8.jar
MD5: f41992ab2729b1cb9c6b4721465aa4e4
SHA1: 6d212f8ea5d908bc9906e669428b7694dff60785
SHA256:3d66e61734b2ddad6e4b34aaa2382480ad6061e59e5e178e346cc275c0429e57

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:apache:struts:1.3.8 *Confidence*:Highest suppress
- **maven:** org.apache.struts:struts-tiles:1.3.8 *Confidence*:High
- **cpe:** cpe:/a:apache:tiles:1.3.8 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2014-0114 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-20 Improper Input Validation

Apache Commons BeanUtils, as distributed in lib/commons-beanutils-1.8.0.jar in Apache Struts 1.x through 1.3.10 and in other products requiring commons-beanutils through 1.9.2, does not suppress the class property, which allows remote attackers to "manipulate" the ClassLoader and execute arbitrary code via the class parameter, as demonstrated by the passing of this parameter to the getClass method of the ActionForm object in Struts 1.

- BID - 67121
- BUGTRAQ - 20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities

- CONFIRM - http://advisories.mageia.org/MGASA-2014-0219.html
- CONFIRM - http://commons.apache.org/proper/commons-beanutils/javadocs/v1.9.2/RELEASE-NOTES.txt
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21674128
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21674812
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675266
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675387
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675689
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675898
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21675972
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676091
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676110
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676303
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676375
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21676931
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg21677110
- CONFIRM - http://www-01.ibm.com/support/docview.wss?uid=swg27042296
- CONFIRM - http://www.ibm.com/support/docview.wss?uid=swg21675496
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
- CONFIRM - http://www.vmware.com/security/advisories/VMSA-2014-0008.html
- CONFIRM - http://www.vmware.com/security/advisories/VMSA-2014-0012.html
- CONFIRM - https://access.redhat.com/solutions/869353
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1091938
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1116665
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05324755
- CONFIRM - https://issues.apache.org/jira/browse/BEANUTILS-463
- CONFIRM - https://security.netapp.com/advisory/ntap-20140911-0001/
- CONFIRM - https://security.netapp.com/advisory/ntap-20180629-0006/
- DEBIAN - DSA-2940
- FEDORA - FEDORA-2014-9380
- FULLDISC - 20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
- GENTOO - GLSA-201607-09
- HP - HPSBGN03041
- HP - HPSBMU03090
- HP - HPSBST03160
- MANDRIVA - MDVSA-2014:095
- MLIST - [apache-ignite-developers] 20180601 [CVE-2014-0114]: Apache Ignite is vulnerable to existing CVE-2014-0114
- MLIST - [oss-security] 20140616 CVE request for commons-beanutils: 'class' property is exposed, potentially leading to RCE
- MLIST - [oss-security] 20140707 Re: CVE request for commons-beanutils: 'class' property is exposed, potentially leading to RCE
- SECUNIA - 57477
- SECUNIA - 58710
- SECUNIA - 58947
- SECUNIA - 59118
- SECUNIA - 59228
- SECUNIA - 59245
- SECUNIA - 59246
- SECUNIA - 59430
- SECUNIA - 59464
- SECUNIA - 59479
- SECUNIA - 59480
- SECUNIA - 59718

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:struts:1.3.8
- ...

CVE-2015-0899 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-20 Improper Input Validation

The MultiPageValidator implementation in Apache Struts 1 1.1 through 1.3.10 allows remote attackers to bypass intended access restrictions via a modified page parameter.

- BID - 74423
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - https://en.osdn.jp/projects/terasoluna/wiki/StrutsPatch2-EN
- CONFIRM - https://security.netapp.com/advisory/ntap-20180629-0006/
- DEBIAN - DSA-3536
- JVN - JVN#86448949
- JVNDB - JVNDB-2015-000042

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:struts:1.3.8
- ...

CVE-2016-1181 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

ActionServlet.java in Apache Struts 1 1.x through 1.3.10 mishandles multithreaded access to an ActionForm instance, which allows remote attackers to execute arbitrary code or cause a denial of service (unexpected memory access) via a multipart request, a related issue to CVE-2015-0899.

- BID - 91068
- BID - 91787
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html

- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1343538
- CONFIRM - https://github.com/kawasima/struts1-forever/commit/eda3a79907ed8fcb0387a0496d0cb14332f250e8
- CONFIRM - https://security-tracker.debian.org/tracker/CVE-2016-1181
- CONFIRM - https://security.netapp.com/advisory/ntap-20180629-0006/
- JVN - JVN#03188560
- JVNDB - JVNDB-2016-000096
- SECTRACK - 1036056

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:struts:1.3.8
- ...

CVE-2016-1182 suppress

Severity:Medium
CVSS Score: 6.4 (AV:N/AC:L/Au:N/C:N/I:P/A:P)
CWE: CWE-20 Improper Input Validation

ActionServlet.java in Apache Struts 1 1.x through 1.3.10 does not properly restrict the Validator configuration, which allows remote attackers to conduct cross-site scripting (XSS) attacks or cause a denial of service via crafted input, a related issue to CVE-2015-0899.

- BID - 91067
- BID - 91787
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1343540
- CONFIRM - https://github.com/kawasima/struts1-forever/commit/eda3a79907ed8fcb0387a0496d0cb14332f250e8
- CONFIRM - https://security-tracker.debian.org/tracker/CVE-2016-1182
- CONFIRM - https://security.netapp.com/advisory/ntap-20180629-0006/
- JVN - JVN#65044642
- JVNDB - JVNDB-2016-000097
- SECTRACK - 1036056

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:struts:1.3.8
- ...

httpclient-4.3.1.jar

Description:

HttpComponents Client

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\chartsearch\lib\httpclient-4.3.1.jar
MD5: 36f69d49a209a0c69df42b80d6159566
SHA1: 0ec13f6423eb6d5858e229939a2bc118473ef94c
SHA256:b3285b0eb7a5c9775467a083e920e95feb99608a20e04c4ceaa521518c4e9a2d

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:apache:httpclient:4.3.1 *Confidence*:Highest suppress
- **maven:** org.apache.httpcomponents:httpclient:4.3.1 *Confidence*:High

Published Vulnerabilities

CVE-2014-3577 suppress

Severity:Medium
CVSS Score: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

org.apache.http.conn.ssl.AbstractVerifier in Apache HttpComponents HttpClient before 4.3.5 and HttpAsyncClient before 4.0.2 does not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a "CN=" string in a field in the distinguished name (DN) of a certificate, as demonstrated by the "foo,CN=www.apache.org" string in the O field.

- BID - 69258
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://access.redhat.com/solutions/1165533

- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05103564
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05363782
- FULLDISC - 20140818 CVE-2014-3577: Apache HttpComponents client: Hostname verification susceptible to MITM attack
- MISC - http://packetstormsecurity.com/files/127913/Apache-HttpComponents-Man-In-The-Middle.html
- OSVDB - 110143
- REDHAT - RHSA-2014:1146
- REDHAT - RHSA-2014:1166
- REDHAT - RHSA-2014:1833
- REDHAT - RHSA-2014:1834
- REDHAT - RHSA-2014:1835
- REDHAT - RHSA-2014:1836
- REDHAT - RHSA-2014:1891
- REDHAT - RHSA-2014:1892
- REDHAT - RHSA-2015:0125
- REDHAT - RHSA-2015:0158
- REDHAT - RHSA-2015:0675
- REDHAT - RHSA-2015:0720
- REDHAT - RHSA-2015:0765
- REDHAT - RHSA-2015:0850
- REDHAT - RHSA-2015:0851
- REDHAT - RHSA-2015:1176
- REDHAT - RHSA-2015:1177
- REDHAT - RHSA-2015:1888
- REDHAT - RHSA-2016:1773
- REDHAT - RHSA-2016:1931
- SECTRACK - 1030812
- SECUNIA - 60466
- UBUNTU - USN-2769-1
- XF - apache-cve20143577-spoofing(95327)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:httpclient:4.3.1
- ...

CVE-2015-5262 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE: CWE-399 Resource Management Errors

http/conn/ssl/SSLConnectionSocketFactory.java in Apache HttpComponents HttpClient before 4.3.6 ignores the http.socket.timeout configuration setting during an SSL handshake, which allows remote attackers to cause a denial of service (HTTPS call hang) via unspecified vectors.

- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1626784
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1261538
- CONFIRM - https://issues.apache.org/jira/browse/HTTPCLIENT-1478
- CONFIRM - https://jenkins.io/security/advisory/2018-02-26/
- FEDORA - FEDORA-2015-15588
- FEDORA - FEDORA-2015-15589
- FEDORA - FEDORA-2015-15590
- SECTRACK - 1033743
- UBUNTU - USN-2769-1

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:httpclient:4.3.1
- ...

spring-core-4.1.4.RELEASE.jar

Description:

Spring Core

License:

The Apache Software License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\tomcat\webapps\openmrs-standalone\WEB-INF\lib\spring-core-4.1.4.RELEASE.jar
MD5: 9c61691672f58e2112461fd832972b81
SHA1: 8df582421867cf7298658e00cd2e9e460b697b05
SHA256:9a6a7d2e520da79db45dbfc3b901d8384e06dfa77b3b36735ad9b790ad10ed88

Evidence

Related Dependencies

Identifiers

- **maven:** org.springframework:spring-core:4.1.4.RELEASE ✓ *Confidence*:Highest
- **cpe:** cpe:/a:pivotal:spring_framework:4.1.4 *Confidence*:Low suppress
- **cpe:** cpe:/a:pivotal_software:spring_framework:4.1.4 *Confidence*:Highest suppress

Published Vulnerabilities

CVE-2015-0201 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-254 7PK - Security Features

The Java SockJS client in Pivotal Spring Framework 4.1.x before 4.1.5 generates predictable session ids, which allows remote attackers to send messages to other sessions via unspecified vectors.

- CONFIRM - https://pivotal.io/security/cve-2015-0201

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal_software:spring_framework:4.1.4
- ...

CVE-2015-3192 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE: CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

Pivotal Spring Framework before 3.2.14 and 4.x before 4.1.7 do not properly process inline DTD declarations when DTD is not entirely disabled, which allows remote attackers to cause a denial of service (memory consumption and out-of-memory errors) via a crafted XML file.

- BID - 90853
- CONFIRM - http://pivotal.io/security/cve-2015-3192
- CONFIRM - https://jira.spring.io/browse/SPR-13136
- FEDORA - FEDORA-2015-11165
- FEDORA - FEDORA-2015-11184
- REDHAT - RHSA-2016:1218
- REDHAT - RHSA-2016:1219
- REDHAT - RHSA-2016:1592
- REDHAT - RHSA-2016:1593
- REDHAT - RHSA-2016:2035
- REDHAT - RHSA-2016:2036
- SECTRACK - 1036587

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal_software:spring_framework:4.1.4
- ...

CVE-2015-5211 suppress

Severity:High
CVSS Score: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
CWE: CWE-20 Improper Input Validation

Under some situations, the Spring Framework 4.2.0 to 4.2.1, 4.0.0 to 4.1.7, 3.2.0 to 3.2.14 and older unsupported versions is vulnerable to a Reflected File Download (RFD) attack. The attack involves a malicious user crafting a URL with a batch script extension that results in the response being downloaded rather than rendered and also includes some input reflected in the response.

- CONFIRM - https://pivotal.io/security/cve-2015-5211
- MISC - https://www.trustwave.com/Resources/SpiderLabs-Blog/Reflected-File-Download---A-New-Web-Attack-Vector/

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal_software:spring_framework:4.1.4
- ...

CVE-2016-5007 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-264 Permissions, Privileges, and Access Controls

Both Spring Security 3.2.x, 4.0.x, 4.1.0 and the Spring Framework 3.2.x, 4.0.x, 4.1.x, 4.2.x rely on URL pattern mappings for authorization and for mapping requests to controllers respectively. Differences in the strictness of the pattern matching mechanisms, for example with regards to space trimming in path segments, can lead Spring Security to not recognize certain paths as not protected that are in fact mapped to Spring MVC controllers that should be protected. The problem is compounded by the fact that the Spring Framework provides richer features with regards to pattern matching as well as by the fact that pattern matching in each Spring Security and the Spring Framework can easily be customized creating additional differences.

- BID - 91687
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - https://pivotal.io/security/cve-2016-5007

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal_software:spring_framework:4.1.4
- ...

CVE-2018-1270 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-358 Improperly Implemented Security Check for Standard

Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 and older unsupported versions, allow applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a remote code execution attack.

- BID - 103696

- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://pivotal.io/security/cve-2018-1270
- EXPLOIT-DB - 44796

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal_software:spring_framework:4.2.9 and all previous versions
- ...

CVE-2018-1271 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 and older unsupported versions, allow applications to configure Spring MVC to serve static resources (e.g. CSS, JS, images). When static resources are served from a file system on Windows (as opposed to the classpath, or the ServletContext), a malicious user can send a request using a specially crafted URL that can lead a directory traversal attack.

- BID - 103699
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://pivotal.io/security/cve-2018-1271
- REDHAT - RHSA-2018:1320

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal_software:spring_framework:4.2.9 and all previous versions
- ...

CVE-2018-1272 suppress

Severity:Medium
CVSS Score: 6.0 (AV:N/AC:M/Au:S/C:P/I:P/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 and older unsupported versions, provide client-side support for multipart requests. When Spring MVC or Spring WebFlux server application (server A) receives input from a remote client, and then uses that input to make a multipart request to another server (server B), it can be exposed to an attack, where an extra multipart is inserted in the content of the request from server A, causing server B to use the wrong value for a part it expects. This could to lead privilege escalation, for example, if the part content represents a username or user roles.

- BID - 103697
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://pivotal.io/security/cve-2018-1272
- MISC - https://exchange.xforce.ibmcloud.com/vulnerabilities/141286
- REDHAT - RHSA-2018:1320

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal_software:spring_framework:4.2.9 and all previous versions
- ...

serialization.xstream.jar

Description:

OpenMRS module project for Serialization Xstream

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\serialization.xstream\serialization.xstream.jar
MD5: 54afd62615ee559450aea84ef085e940
SHA1: de0dbe9527309f96cdb6704287dc9e5f78d1905f
SHA256:29e820eaea44de4019d2b2f268faec4aae82c33b0468fbbaa6ebabd3c7095280

Evidence

Identifiers

- **cpe:** cpe:/a:xstream_project:xstream:0.2.14 *Confidence*:Low suppress
- **maven:** org.openmrs.module:serialization.xstream-omod:0.2.14 *Confidence*:High

Published Vulnerabilities

CVE-2016-3674 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-200 Information Exposure

Multiple XML external entity (XXE) vulnerabilities in the (1) Dom4JDriver, (2) DomDriver, (3) JDomDriver, (4) JDom2Driver, (5) SjsxpDriver, (6) StandardStaxDriver, and (7) WstxDriver drivers in XStream before 1.4.9 allow remote attackers to read arbitrary files via a crafted XML document.

- BID - 85381
- CONFIRM - http://x-stream.github.io/changes.html#1.4.9
- CONFIRM - https://github.com/x-stream/xstream/issues/25
- DEBIAN - DSA-3575

- FEDORA - FEDORA-2016-250042b8a6
- FEDORA - FEDORA-2016-de909cc333
- MLIST - [oss-security] 20160325 CVE request - XStream: XXE vulnerability
- MLIST - [oss-security] 20160328 Re: CVE request - XStream: XXE vulnerability
- REDHAT - RHSA-2016:2822
- REDHAT - RHSA-2016:2823
- SECTRACK - 1036419

Vulnerable Software & Versions:

- cpe:/a:xstream_project:xstream:1.4.8 and all previous versions

CVE-2017-7957 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-20 Improper Input Validation

XStream through 1.4.9, when a certain denyTypes workaround is not used, mishandles attempts to create an instance of the primitive type 'void' during unmarshalling, leading to a remote application crash, as demonstrated by an xstream.fromXML("<void/>") call.

- BID - 100687
- CONFIRM - http://x-stream.github.io/CVE-2017-7957.html
- CONFIRM - https://www-prd-trops.events.ibm.com/node/715749
- DEBIAN - DSA-3841
- REDHAT - RHSA-2017:1832
- REDHAT - RHSA-2017:2888
- REDHAT - RHSA-2017:2889
- SECTRACK - 1039499
- XF - xstream-cve20177957-dos(125800)

Vulnerable Software & Versions:

- cpe:/a:xstream_project:xstream:1.4.9 and all previous versions

htmlwidgets-api-1.9.0.jar

Description:

API project for HTML Widgets

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\htmlwidgets\lib\htmlwidgets-api-1.9.0.jar
MD5: 34549a156f811871e5e4324234e21f86
SHA1: fc14e53aa2b80724a71d2ee5672a68c6facc82e1
SHA256:315d747c11ca1e3c479dc76ff31e00fb1b2dbcbffaab18683c74004231de508b

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:widgets_project:widgets:1.9.0 *Confidence*:Low suppress
- **maven:** org.openmrs.module:htmlwidgets-api:1.9.0 *Confidence*:High

Published Vulnerabilities

CVE-2015-6737 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in the Widgets extension for MediaWiki allows remote attackers to inject arbitrary web script or HTML via vectors involving base64 encoded content.

- BID - 76858
- FEDORA - FEDORA-2015-13920
- GENTOO - GLSA-201510-05
- MLIST - [MediaWiki-announce] 20150810 MediaWiki Security and Maintenance Releases: 1.25.2, 1.24.3, 1.23.10
- MLIST - [oss-security] 20150812 CVE Request: MediaWiki 1.25.2, 1.24.3, 1.23.10
- MLIST - [oss-security] 20150827 Re: CVE Request: MediaWiki 1.25.2, 1.24.3, 1.23.10

Vulnerable Software & Versions:

- cpe:/a:widgets_project:widgets:-::~~~mediawiki~~

spring-jms-3.0.5.RELEASE.jar

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\event\lib\spring-jms-3.0.5.RELEASE.jar
MD5: 181faf34f324eb6a8c2d56f61f184b99
SHA1: 5a880fd07605747e5a641f78fd8039a761c5865e
SHA256:0eacece0d6d613665fc84f6a428c0a9422f2b195f91daa132da1029154ba906b

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:vmware:springsource_spring_framework:3.0.5 *Confidence*:Highest suppress
- **maven:** org.springframework:spring-jms:3.0.5.RELEASE ✓ *Confidence*:Highest
- **cpe:** cpe:/a:pivotal:spring_framework:3.0.5 *Confidence*:Highest suppress
- **cpe:** cpe:/a:pivotal_software:spring_framework:3.0.5 *Confidence*:Highest suppress
- **cpe:** cpe:/a:springsource:spring_framework:3.0.5 *Confidence*:Highest suppress

Published Vulnerabilities

CVE-2011-2730 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-16 Configuration

VMware SpringSource Spring Framework before 2.5.6.SEC03, 2.5.7.SR023, and 3.x before 3.0.6, when a container supports Expression Language (EL), evaluates EL expressions in tags twice, which allows remote attackers to obtain sensitive information via a (1) name attribute in a (a) spring:hasBindErrors tag; (2) path attribute in a (b) spring:bind or (c) spring:nestedpath tag; (3) arguments, (4) code, (5) text, (6) var, (7) scope, or (8) message attribute in a (d) spring:message or (e) spring:theme tag; or (9) var, (10) scope, or (11) value attribute in a (f) spring:transform tag, aka "Expression Language Injection."

- CONFIRM - http://support.springsource.com/security/cve-2011-2730
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
- DEBIAN - DSA-2504
- MISC - http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=677814
- MISC - https://docs.google.com/document/d/1dc1xxO8UMFaGLOwgkykYdghGWm_2Gn0iCrxFsympqcE/edit
- REDHAT - RHSA-2013:0191
- REDHAT - RHSA-2013:0192
- REDHAT - RHSA-2013:0193
- REDHAT - RHSA-2013:0194
- REDHAT - RHSA-2013:0195
- REDHAT - RHSA-2013:0196
- REDHAT - RHSA-2013:0197
- REDHAT - RHSA-2013:0198
- REDHAT - RHSA-2013:0221
- REDHAT - RHSA-2013:0533
- SECTRACK - 1029151

Vulnerable Software & Versions: (show all)

- cpe:/a:springsource:spring_framework:3.0.5 and all previous versions
- ...

CVE-2011-2894 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

Spring Framework 3.0.0 through 3.0.5, Spring Security 3.0.0 through 3.0.5 and 2.0.0 through 2.0.6, and possibly other versions deserialize objects from untrusted sources, which allows remote attackers to bypass intended security restrictions and execute untrusted code by (1) serializing a java.lang.Proxy instance and using InvocationHandler, or (2) accessing internal AOP interfaces, as demonstrated using deserialization of a DefaultListableBeanFactory instance to execute arbitrary commands via the java.lang.Runtime class.

- BID - 49536
- BUGTRAQ - 20110909 CVE-2011-2894: Spring Framework and Spring Security serialization-based remoting vulnerabilities
- CONFIRM - http://www.springsource.com/security/cve-2011-2894
- REDHAT - RHSA-2011:1334
- SREASON - 8405
- XF - spring-framework-object-sec-bypass(69687)

Vulnerable Software & Versions: (show all)

- cpe:/a:vmware:springsource_spring_framework:3.0.5
- ...

CVE-2013-4152 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

The Spring OXM wrapper in Spring Framework before 3.2.4 and 4.0.0.M1, when using the JAXB marshaller, does not disable entity resolution, which allows context-dependent attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via an XML external entity declaration in conjunction with an entity

reference in a (1) DOMSource, (2) StAXSource, (3) SAXSource, or (4) StreamSource, aka an XML External Entity (XXE) issue.

- BID - 61951
- BUGTRAQ - 20130822 CVE-2013-4152 XML External Entity (XXE) injection in Spring Framework
- CONFIRM - http://www.gopivotal.com/security/cve-2013-4152
- CONFIRM - https://github.com/spring-projects/spring-framework/pull/317/files
- CONFIRM - https://jira.springsource.org/browse/SPR-10806
- DEBIAN - DSA-2842
- FULLDISC - 20131102 XXE Injection in Spring Framework
- REDHAT - RHSA-2014:0212
- REDHAT - RHSA-2014:0245
- REDHAT - RHSA-2014:0254
- REDHAT - RHSA-2014:0400

Vulnerable Software & Versions: (show all)

- cpe:/a:springsource:spring_framework:3.0.5
- ...

CVE-2013-6429 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

The SourceHttpMessageConverter in Spring MVC in Spring Framework before 3.2.5 and 4.0.0.M1 through 4.0.0.RC1 does not disable external entity resolution, which allows remote attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML, aka an XML External Entity (XXE) issue, and a different vulnerability than CVE-2013-4152 and CVE-2013-7315.

- BID - 64947
- BUGTRAQ - 20140114 CVE-2013-6429 Fix for XML External Entity (XXE) injection (CVE-2013-4152) in Spring Framework was incomplete
- CONFIRM - http://www.gopivotal.com/security/cve-2013-6429
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05324755
- CONFIRM - https://jira.springsource.org/browse/SPR-11078?page=com.atlassian.jira.plugin.system.issuetabpanels:worklog-tabpanel
- REDHAT - RHSA-2014:0400

Vulnerable Software & Versions: (show all)

- cpe:/a:springsource:spring_framework:3.0.5
- ...

CVE-2013-7315 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

The Spring MVC in Spring Framework before 3.2.4 and 4.0.0.M1 through 4.0.0.M2 does not disable external entity resolution for the StAX XMLInputFactory, which allows context-dependent attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML with JAXB, aka an XML External Entity (XXE) issue, and a different vulnerability than CVE-2013-4152. NOTE: this issue was SPLIT from CVE-2013-4152 due to different affected versions.

- BID - 77998
- BUGTRAQ - 20130822 CVE-2013-4152 XML External Entity (XXE) injection in Spring Framework
- CONFIRM - http://www.gopivotal.com/security/cve-2013-4152
- CONFIRM - https://jira.springsource.org/browse/SPR-10806
- DEBIAN - DSA-2842
- FULLDISC - 20131102 XXE Injection in Spring Framework

Vulnerable Software & Versions: (show all)

- cpe:/a:springsource:spring_framework:3.0.5
- ...

CVE-2014-0054 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-352 Cross-Site Request Forgery (CSRF)

The Jaxb2RootElementHttpMessageConverter in Spring MVC in Spring Framework before 3.2.8 and 4.0.0 before 4.0.2 does not disable external entity resolution, which allows remote attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML, aka an XML External Entity (XXE) issue. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4152, CVE-2013-7315, and CVE-2013-6429.

- BID - 66148
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - https://jira.spring.io/browse/SPR-11376
- REDHAT - RHSA-2014:0400

Vulnerable Software & Versions: (show all)

- cpe:/a:springsource:spring_framework:3.0.5
- ...

CVE-2014-0225 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-611 Improper Restriction of XML External Entity Reference ('XXE')

When processing user provided XML documents, the Spring Framework 4.0.0 to 4.0.4, 3.0.0 to 3.2.8, and possibly earlier unsupported versions did not disable by default the resolution of URI references in a DTD declaration. This enabled an XXE attack.

- CONFIRM - https://pivotal.io/security/cve-2014-0225

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal_software:spring_framework:3.0.5
- ...

CVE-2014-1904 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in web/servlet/tags/form/FormTag.java in Spring MVC in Spring Framework 3.0.0 before 3.2.8 and 4.0.0 before 4.0.2 allows remote attackers to inject arbitrary web script or HTML via the requested URI in a default action.

- BID - 66137
- BUGTRAQ - 20140311 CVE-2014-1904 XSS when using Spring MVC
- CONFIRM - http://docs.spring.io/spring/docs/3.2.8.RELEASE/changelog.txt
- CONFIRM - http://www.gopivotal.com/security/cve-2014-1904
- CONFIRM - https://github.com/spring-projects/spring-framework/commit/741b4b229ae032bd17175b46f98673ce0bd2d485
- CONFIRM - https://jira.springsource.org/browse/SPR-11426
- FULLDISC - 20140312 CVE-2014-1904 XSS when using Spring MVC
- REDHAT - RHSA-2014:0400

Vulnerable Software & Versions: (show all)

- cpe:/a:springsource:spring_framework:3.0.5
- ...

CVE-2014-3578 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Directory traversal vulnerability in Pivotal Spring Framework 3.x before 3.2.9 and 4.0 before 4.0.5 allows remote attackers to read arbitrary files via a crafted URL.

- BID - 68042
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1131882
- JVN - JVN#49154900
- JVNDB - JVNDB-2014-000054
- MISC - http://pivotal.io/security/cve-2014-3578
- REDHAT - RHSA-2015:0234
- REDHAT - RHSA-2015:0235
- REDHAT - RHSA-2015:0720

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal:spring_framework:3.0.5
- ...

CVE-2014-3625 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Directory traversal vulnerability in Pivotal Spring Framework 3.0.4 through 3.2.x before 3.2.12, 4.0.x before 4.0.8, and 4.1.x before 4.1.2 allows remote attackers to read arbitrary files via unspecified vectors, related to static resource handling.

- CONFIRM - http://www.pivotal.io/security/cve-2014-3625
- CONFIRM - https://jira.spring.io/browse/SPR-12354
- REDHAT - RHSA-2015:0236
- REDHAT - RHSA-2015:0720

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal:spring_framework:3.0.5
- ...

CVE-2016-9878 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

An issue was discovered in Pivotal Spring Framework before 3.2.18, 4.2.x before 4.2.9, and 4.3.x before 4.3.5. Paths provided to the ResourceServlet were not properly sanitized and as a result exposed to directory traversal attacks.

- BID - 95072
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://pivotal.io/security/cve-2016-9878
- CONFIRM - https://security.netapp.com/advisory/ntap-20180419-0002/
- REDHAT - RHSA-2017:3115
- SECTRACK - 1040698

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal_software:spring_framework:3.2.0 and all previous versions
- ...

CVE-2018-1270 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-358 Improperly Implemented Security Check for Standard

Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 and older unsupported versions, allow applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a remote code execution attack.

- BID - 103696
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html

- CONFIRM - https://pivotal.io/security/cve-2018-1270
- EXPLOIT-DB - 44796

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal_software:spring_framework:4.2.9 and all previous versions
- ...

CVE-2018-1271 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 and older unsupported versions, allow applications to configure Spring MVC to serve static resources (e.g. CSS, JS, images). When static resources are served from a file system on Windows (as opposed to the classpath, or the ServletContext), a malicious user can send a request using a specially crafted URL that can lead a directory traversal attack.

- BID - 103699
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://pivotal.io/security/cve-2018-1271
- REDHAT - RHSA-2018:1320

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal_software:spring_framework:4.2.9 and all previous versions
- ...

CVE-2018-1272 suppress

Severity:Medium
CVSS Score: 6.0 (AV:N/AC:M/Au:S/C:P/I:P/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 and older unsupported versions, provide client-side support for multipart requests. When Spring MVC or Spring WebFlux server application (server A) receives input from a remote client, and then uses that input to make a multipart request to another server (server B), it can be exposed to an attack, where an extra multipart is inserted in the content of the request from server A, causing server B to use the wrong value for a part it expects. This could to lead privilege escalation, for example, if the part content represents a username or user roles.

- BID - 103697
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://pivotal.io/security/cve-2018-1272
- MISC - https://exchange.xforce.ibmcloud.com/vulnerabilities/141286
- REDHAT - RHSA-2018:1320

Vulnerable Software & Versions: (show all)

- cpe:/a:pivotal_software:spring_framework:4.2.9 and all previous versions
- ...

appui-api-1.8.0.jar

Description:

API project for AppUI

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\appui\lib\appui-api-1.8.0.jar
MD5: 715041a85a7e6442068f48f529536636
SHA1: e153026cc9f5cc2400034da6d59b4ac41ba4af2a
SHA256:04a5d259331522fc07e8f30a8b07890440a9f59fa9be38841ecd3fe7eaf85b61

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:app_project:app:1.8.0 *Confidence*:Low suppress
- **maven:** org.openmrs.module:appui-api:1.8.0 *Confidence*:High

Published Vulnerabilities

CVE-2018-13661 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-190 Integer Overflow or Wraparound

The mintToken function of a smart contract implementation for APP, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value.

- MISC - https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md

- MISC - https://github.com/BlockChainsSecurity/EtherTokens/tree/master/APP

Vulnerable Software & Versions:

- cpe:/a:app_project:app:-

jackson-databind-2.9.0.jar

Description:

General data-binding functionality for Jackson: works on core streaming API

License:

http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\tomcat\webapps\openmrs-standalone\WEB-INF\lib\jackson-databind-2.9.0.jar
MD5: bc9edd751df7dbe30d4c68a1662c3de
SHA1: 14fb5f088cc0b0dc90a73ba745bcade4961a3ee3
SHA256:02b20e2a73d5539b8c6898e1ade73623c5b555a3bcd46308410a9179c8c5d455

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:fasterxml:jackson-databind:2.9.0 *Confidence*:Highest suppress
- **maven:** com.fasterxml.jackson.core:jackson-databind:2.9.0 *Confidence*:High
- **cpe:** cpe:/a:fasterxml:jackson:2.9.0 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2017-15095 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-502 Deserialization of Untrusted Data

A deserialization flaw was discovered in the jackson-databind in versions before 2.8.10 and 2.9.1, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper. This issue extends the previous flaw CVE-2017-7525 by blacklisting more classes that could be used maliciously.

- BID - 103880
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1680
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1737
- CONFIRM - https://security.netapp.com/advisory/ntap-20171214-0003/
- DEBIAN - DSA-4037
- REDHAT - RHSA-2017:3189
- REDHAT - RHSA-2017:3190
- REDHAT - RHSA-2018:0342
- REDHAT - RHSA-2018:0478
- REDHAT - RHSA-2018:0479
- REDHAT - RHSA-2018:0480
- REDHAT - RHSA-2018:0481
- REDHAT - RHSA-2018:0576
- REDHAT - RHSA-2018:0577
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451
- SECTRACK - 1039769

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.9.0
- ...

CVE-2018-5968 suppress

Severity:Medium
CVSS Score: 5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
CWE: CWE-184 Incomplete Blacklist

FasterXML jackson-databind through 2.8.11 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 and CVE-2017-17485 deserialization flaws. This is exploitable via two different gadgets that bypass a blacklist.

- CONFIRM - https://security.netapp.com/advisory/ntap-20180423-0002/

- DEBIAN - DSA-4114
- MISC - https://github.com/FasterXML/jackson-databind/issues/1899
- REDHAT - RHSA-2018:0478
- REDHAT - RHSA-2018:0479
- REDHAT - RHSA-2018:0480
- REDHAT - RHSA-2018:0481
- REDHAT - RHSA-2018:1525

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.9.0
- ...

CVE-2018-7489 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-184 Incomplete Blacklist

FasterXML jackson-databind before 2.8.11.1 and 2.9.x before 2.9.5 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the c3p0 libraries are available in the classpath.

- BID - 103203
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1931
- CONFIRM - https://security.netapp.com/advisory/ntap-20180328-0001/
- DEBIAN - DSA-4190
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451
- REDHAT - RHSA-2018:1786
- REDHAT - RHSA-2018:2088
- REDHAT - RHSA-2018:2089
- REDHAT - RHSA-2018:2090
- SECTRACK - 1040693

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.9.0
- ...

activemq-protobuf-1.1.jar

Description:

A Simpler Protocol Buffer Java API. Includes a Proto to Java compiler.

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\event\lib\activemq-protobuf-1.1.jar
MD5: 38add15a7775073053fe3aa81979336c
SHA1: 26682eb801f70563511f7c424dc10e8b3e66340e
SHA256:8323444e48a1920afe37b5f24b6dc139f35793e8a87fa178f6d9c8f92a6f39d1

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:apache:activemq:1.1 *Confidence*:Highest suppress
- **maven:** org.apache.activemq.protobuf:activemq-protobuf:1.1 *Confidence*:High

Published Vulnerabilities

CVE-2010-0684 suppress

Severity:Low
CVSS Score: 3.5 (AV:N/AC:M/Au:S/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in createDestination.action in Apache ActiveMQ before 5.3.1 allows remote authenticated users to inject arbitrary web script or HTML via the JMSDestination parameter in a queue action.

- BID - 39119
- BUGTRAQ - 20100330 CVE-2010-0684: Apache ActiveMQ Persistent Cross-Site Scripting (XSS) Vulnerability
- CONFIRM - http://activemq.apache.org/activemq-531-release.html

- CONFIRM - https://issues.apache.org/activemq/browse/AMQ-2613
- CONFIRM - https://issues.apache.org/activemq/browse/AMQ-2625
- MISC - http://www.rajatswarup.com/CVE-2010-0684.txt
- SECTRACK - 1023778
- XF - activemq-createdestination-xss(57397)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:1.1
- ...

CVE-2010-1244 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-352 Cross-Site Request Forgery (CSRF)

Cross-site request forgery (CSRF) vulnerability in createDestination.action in Apache ActiveMQ before 5.3.1 allows remote attackers to hijack the authentication of unspecified victims for requests that create queues via the JMSDestination parameter in a queue action.

- CONFIRM - http://activemq.apache.org/activemq-531-release.html
- CONFIRM - https://issues.apache.org/activemq/browse/AMQ-2613
- CONFIRM - https://issues.apache.org/activemq/browse/AMQ-2625
- XF - activemq-web-console-csrf(57398)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:1.1
- ...

CVE-2011-4905 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-399 Resource Management Errors

Apache ActiveMQ before 5.6.0 allows remote attackers to cause a denial of service (file-descriptor exhaustion and broker crash or hang) by sending many openwire failover:tcp:// connection requests.

- BID - 50904
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1209700
- CONFIRM - http://svn.apache.org/viewvc?view=revision&revision=1211844
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-3294
- MLIST - [oss-security] 20111224 CVE Request for Apache ActiveMQ DoS
- MLIST - [oss-security] 20111225 Re: CVE Request for Apache ActiveMQ DoS

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:1.1
- ...

CVE-2012-5784 suppress

Severity:Medium
CVSS Score: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)
CWE: CWE-20 Improper Input Validation

Apache Axis 1.4 and earlier, as used in PayPal Payments Pro, PayPal Mass Pay, PayPal Transactional Information SOAP, the Java Message Service implementation in Apache ActiveMQ, and other products, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- BID - 56408
- MISC - http://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf
- REDHAT - RHSA-2013:0269
- REDHAT - RHSA-2013:0683
- REDHAT - RHSA-2014:0037
- XF - apache-axis-ssl-spoofing(79829)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2012-6092 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Multiple cross-site scripting (XSS) vulnerabilities in the web demos in Apache ActiveMQ before 5.8.0 allow remote attackers to inject arbitrary web script or HTML via (1) the refresh parameter to PortfolioPublishServlet.java (aka demo/portfolioPublish or Market Data Publisher), or vectors involving (2) debug logs or (3) subscribe messages in webapp/websocket/chat.js. NOTE: AMQ-4124 is covered by CVE-2012-6551.

- BID - 59400
- CONFIRM - http://activemq.apache.org/activemq-580-release.html
- CONFIRM - https://fisheye6.atlassian.com/changelog/activemq?cs=1399577
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4115
- CONFIRM - https://issues.apache.org/jira/secure/ReleaseNote.jspa?projectId=12311210&version=12323282
- REDHAT - RHSA-2013:1029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2012-6551 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-399 Resource Management Errors

The default configuration of Apache ActiveMQ before 5.8.0 enables a sample web application, which allows remote attackers to cause a denial of service (broker resource consumption) via HTTP requests.

- BID - 59401
- CONFIRM - http://activemq.apache.org/activemq-580-release.html
- CONFIRM - https://fisheye6.atlassian.com/changelog/activemq?cs=1404998
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4124
- CONFIRM - https://issues.apache.org/jira/secure/ReleaseNote.jspa?projectId=12311210&version=12323282
- MLIST - [dev] 20121022 [DISCUSS] - ActiveMQ out of the box - Should not include the demos
- REDHAT - RHSA-2013:1029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2013-1879 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in scheduled.jsp in Apache ActiveMQ 5.8.0 and earlier allows remote attackers to inject arbitrary web script or HTML via vectors involving the "cron of a message."

- BID - 61142
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4397
- REDHAT - RHSA-2013:1029
- XF - activemq-cve20131879-xss(85586)

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.8.0 and all previous versions
- ...

CVE-2013-1880 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in the Portfolio publisher servlet in the demo web application in Apache ActiveMQ before 5.9.0 allows remote attackers to inject arbitrary web script or HTML via the refresh parameter to demo/portfolioPublish, a different vulnerability than CVE-2012-6092.

- BID - 65615
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=924447
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4398
- REDHAT - RHSA-2013:1029

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.8.0 and all previous versions
- ...

CVE-2013-3060 suppress

Severity:Medium
CVSS Score: 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)
CWE: CWE-287 Improper Authentication

The web console in Apache ActiveMQ before 5.8.0 does not require authentication, which allows remote attackers to obtain sensitive information or cause a denial of service via HTTP requests.

- BID - 59402
- CONFIRM - http://activemq.apache.org/activemq-580-release.html
- CONFIRM - https://fisheye6.atlassian.com/changelog/activemq?cs=1404998
- CONFIRM - https://issues.apache.org/jira/browse/AMQ-4124
- CONFIRM - https://issues.apache.org/jira/secure/ReleaseNote.jspa?projectId=12311210&version=12323282
- MLIST - [dev] 20121022 [DISCUSS] - ActiveMQ out of the box - Should not include the demos
- REDHAT - RHSA-2013:1029
- REDHAT - RHSA-2013:1221

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.7.0 and all previous versions
- ...

CVE-2014-3576 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-264 Permissions, Privileges, and Access Controls

The processControlCommand function in broker/TransportConnection.java in Apache ActiveMQ before 5.11.0 allows remote attackers to cause a denial of service (shutdown) via a shutdown command.

- BID - 76272
- BUGTRAQ - 20151106 [ANNOUNCE] CVE-2014-3576 - Apache ActiveMQ vulnerabilities
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
- CONFIRM - https://github.com/apache/activemq/commit/00921f2
- DEBIAN - DSA-3330
- MISC - http://packetstormsecurity.com/files/134274/Apache-ActiveMQ-5.10.1-Denial-Of-Service.html
- MLIST - [dev] 20150721 About CVE-2014-3576
- SECTRACK - 1033898

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:activemq:5.10.0 and all previous versions
- ...

CVE-2015-5182 suppress

Severity:Medium
CVSS Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-352 Cross-Site Request Forgery (CSRF)

Cross-site request forgery (CSRF) vulnerability in the jolokia API in A-MQ.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1248809

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:-

CVE-2015-5183 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-254 7PK - Security Features

The Hawtio console in A-MQ does not set HTTPOnly or Secure attributes on cookies.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1249182

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:-

CVE-2015-5184 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-254 7PK - Security Features

The Hawtio console in A-MQ allows remote attackers to obtain sensitive information and perform other unspecified impact.

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1249183

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:-

CVE-2016-3088 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-20 Improper Input Validation

The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.

- CONFIRM - http://activemq.apache.org/security-advisories.data/CVE-2016-3088-announcement.txt
- EXPLOIT-DB - 42283
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-16-356
- MISC - http://www.zerodayinitiative.com/advisories/ZDI-16-357
- REDHAT - RHSA-2016:2036
- SECTRACK - 1035951

Vulnerable Software & Versions:

- cpe:/a:apache:activemq:5.13.3 and all previous versions

registrationapp.jar (shaded: org.openmrs.module:registrationapp-omod:1.12.0)

Description:

OMOD project for RegistrationApp

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\registrationapp\registrationapp.jar\META-INF/maven/org.openmrs.module/registrationapp-omod/pom.xml
MD5: d2c76cdc933c1ebe8dab1a22d5bec7ca
SHA1: 535bbb9e6da7b9d88836f17b04c4bce003b7c859
SHA256:3a8251a249f84aa280aeeff888d1f236748a7f253d7457e525557a2f19be65fb

Evidence

Identifiers

- **maven:** org.openmrs.module:registrationapp-omod:1.12.0 *Confidence*:High
- **cpe:** cpe:/a:app_project:app:1.12.0 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2018-13661 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-190 Integer Overflow or Wraparound

The mintToken function of a smart contract implementation for APP, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value.

- MISC - https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md
- MISC - https://github.com/BlockChainsSecurity/EtherTokens/tree/master/APP

Vulnerable Software & Versions:

- cpe:/a:app_project:app:-

appui.jar (shaded: org.openmrs.module:appui-omod:1.8.0)

Description:

OMOD project for AppUI

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\appui\appui.jar\META-INF/maven/org.openmrs.module/appui-omod/pom.xml
MD5: 423a6b8d7c87c5b7cb056fc5536199e4
SHA1: e797e31a5a7558088919dc01da1095776a87bd99
SHA256:9baa09895af9bd89650d0733e51072bfaa62a5fac67d5293bc2bf0e2c99b7710

Evidence

Identifiers

- **cpe:** cpe:/a:app_project:app:1.8.0 *Confidence*:Low suppress
- **maven:** org.openmrs.module:appui-omod:1.8.0 *Confidence*:High

Published Vulnerabilities

CVE-2018-13661 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-190 Integer Overflow or Wraparound

The mintToken function of a smart contract implementation for APP, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value.

- MISC - https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md
- MISC - https://github.com/BlockChainsSecurity/EtherTokens/tree/master/APP

Vulnerable Software & Versions:

- cpe:/a:app_project:app:-

htmlwidgets.jar (shaded: org.openmrs.module:htmlwidgets-omod:1.9.0)

Description:

OpenMRS module project for HTML Widgets

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\htmlwidgets\htmlwidgets.jar\META-INF/maven/org.openmrs.module/htmlwidgets-omod/pom.xml
MD5: 3fa1bbe831d6f7d6582941873b8722a7
SHA1: 84dc8e3b56cd238fc794b1a42918eb87ea203747
SHA256:c6489595b4106a126ad3af649659b724c20f66f40a5997943d2f522200263e2c

Evidence

Identifiers

- **cpe:** cpe:/a:widgets_project:widgets:1.9.0 *Confidence*:Low suppress
- **maven:** org.openmrs.module:htmlwidgets-omod:1.9.0 *Confidence*:High

Published Vulnerabilities

CVE-2015-6737 suppress

Severity:Medium
CVSS Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Cross-site scripting (XSS) vulnerability in the Widgets extension for MediaWiki allows remote attackers to inject arbitrary web script or HTML via vectors involving base64 encoded content.

- BID - 76858
- FEDORA - FEDORA-2015-13920
- GENTOO - GLSA-201510-05
- MLIST - [MediaWiki-announce] 20150810 MediaWiki Security and Maintenance Releases: 1.25.2, 1.24.3, 1.23.10
- MLIST - [oss-security] 20150812 CVE Request: MediaWiki 1.25.2, 1.24.3, 1.23.10
- MLIST - [oss-security] 20150827 Re: CVE Request: MediaWiki 1.25.2, 1.24.3, 1.23.10

Vulnerable Software & Versions:

- cpe:/a:widgets_project:widgets:-::~~~mediawiki~~

uicommons.jar (shaded: org.openmrs.module:uicommons-scss:2.6.0)

Description:

SCSS that can be shared with other OpenMRS modules that want to build styling based on uicommons

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\appdata\.openmrs-lib-cache\uicommons\uicommons.jar\lib/pom.xml
MD5: 4980fa5f35f82e56735a203c1f44de49
SHA1: c0a411c1eaddad26a3bf542b969c689b2416bc36
SHA256:0309db06831d1fc06ba1a315996fe2a8bf7d2ca5d2c5b31071550992c3b0c95e

Evidence

Identifiers

- **cpe:** cpe:/a:content_project:content:2.6.0 *Confidence*:Low suppress
- **maven:** org.openmrs.module:uicommons-scss:2.6.0 *Confidence*:High

Published Vulnerabilities

CVE-2017-16111 suppress

Severity:Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-400 Uncontrolled Resource Consumption ('Resource Exhaustion')

The content module is a module to parse HTTP Content-* headers. It is used by the hapijs framework to provide this functionality. The module is vulnerable to regular expression denial of service when passed a specifically crafted Content-Type or Content-Disposition header.

- MISC - https://nodesecurity.io/advisories/530

Vulnerable Software & Versions:

- cpe:/a:content_project:content:3.0.5::~~~node.js~~ and all previous versions

ehcache-2.10.0.jar (shaded: com.fasterxml.jackson.core:jackson-databind:2.3.3)

Description:

General data-binding functionality for Jackson: works on core streaming API

File Path: C:\openMRS\referenceapplication-standalone-2.8.0\tomcat\webapps\openmrs-standalone\WEB-INF\lib\ehcache-2.10.0.jar\rest-management-private-classpath/META-INF/maven/com.fasterxml.jackson.core/jackson-databind/pom.xml
MD5: 04e23f17a1150e7ec1f70eeac734af7d
SHA1: fc2fa919676ab9574a7e312fd44741e5569b86a1
SHA256:711e6ba52cbad60347308ff19e464851c2aca09ec50b2a411b14d06d8df9ee84

Evidence

Identifiers

- **cpe:** cpe:/a:fasterxml:jackson-databind:2.3.3 *Confidence*:Highest suppress
- **maven:** com.fasterxml.jackson.core:jackson-databind:2.3.3 *Confidence*:High
- **cpe:** cpe:/a:fasterxml:jackson:2.3.3 *Confidence*:Low suppress

Published Vulnerabilities

CVE-2017-15095 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-502 Deserialization of Untrusted Data

A deserialization flaw was discovered in the jackson-databind in versions before 2.8.10 and 2.9.1, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper. This issue extends the previous flaw CVE-2017-7525 by blacklisting more classes that could be used maliciously.

- BID - 103880
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1680
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1737
- CONFIRM - https://security.netapp.com/advisory/ntap-20171214-0003/
- DEBIAN - DSA-4037
- REDHAT - RHSA-2017:3189
- REDHAT - RHSA-2017:3190
- REDHAT - RHSA-2018:0342
- REDHAT - RHSA-2018:0478
- REDHAT - RHSA-2018:0479
- REDHAT - RHSA-2018:0480
- REDHAT - RHSA-2018:0481
- REDHAT - RHSA-2018:0576
- REDHAT - RHSA-2018:0577
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451
- SECTRACK - 1039769

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.3.3
- ...

CVE-2017-17485 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-94 Improper Control of Generation of Code ('Code Injection')

FasterXML jackson-databind through 2.8.10 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the Spring libraries are available in the classpath.

- BUGTRAQ - 20180109 CVE-2017-17485: one more way of rce in jackson-databind when defaultTyping+objects are used
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1855
- CONFIRM - https://security.netapp.com/advisory/ntap-20180201-0003/
- DEBIAN - DSA-4114
- MISC - https://github.com/irsl/jackson-rce-via-spel/
- REDHAT - RHSA-2018:0116
- REDHAT - RHSA-2018:0342
- REDHAT - RHSA-2018:0478
- REDHAT - RHSA-2018:0479
- REDHAT - RHSA-2018:0480
- REDHAT - RHSA-2018:0481
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.8.10 and all previous versions
- ...

CVE-2017-7525 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-502 Deserialization of Untrusted Data

A deserialization flaw was discovered in the jackson-databind, versions before 2.6.7.1, 2.7.9.1 and 2.8.9, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper.

- BID - 99623
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1462702
- CONFIRM - https://cwiki.apache.org/confluence/display/WW/S2-055
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1599
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1723

- CONFIRM - https://security.netapp.com/advisory/ntap-20171214-0002/
- DEBIAN - DSA-4004
- REDHAT - RHSA-2017:1834
- REDHAT - RHSA-2017:1835
- REDHAT - RHSA-2017:1836
- REDHAT - RHSA-2017:1837
- REDHAT - RHSA-2017:1839
- REDHAT - RHSA-2017:1840
- REDHAT - RHSA-2017:2477
- REDHAT - RHSA-2017:2546
- REDHAT - RHSA-2017:2547
- REDHAT - RHSA-2017:2633
- REDHAT - RHSA-2017:2635
- REDHAT - RHSA-2017:2636
- REDHAT - RHSA-2017:2637
- REDHAT - RHSA-2017:2638
- REDHAT - RHSA-2017:3141
- REDHAT - RHSA-2017:3454
- REDHAT - RHSA-2017:3455
- REDHAT - RHSA-2017:3456
- REDHAT - RHSA-2017:3458
- REDHAT - RHSA-2018:0294
- REDHAT - RHSA-2018:0342
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- SECTRACK - 1039744
- SECTRACK - 1039947
- SECTRACK - 1040360

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.3.3
- ...

CVE-2018-5968 suppress

Severity:Medium
CVSS Score: 5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
CWE: CWE-184 Incomplete Blacklist

FasterXML jackson-databind through 2.8.11 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 and CVE-2017-17485 deserialization flaws. This is exploitable via two different gadgets that bypass a blacklist.

- CONFIRM - https://security.netapp.com/advisory/ntap-20180423-0002/
- DEBIAN - DSA-4114
- MISC - https://github.com/FasterXML/jackson-databind/issues/1899
- REDHAT - RHSA-2018:0478
- REDHAT - RHSA-2018:0479
- REDHAT - RHSA-2018:0480
- REDHAT - RHSA-2018:0481
- REDHAT - RHSA-2018:1525

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.8.11 and all previous versions
- ...

CVE-2018-7489 suppress

Severity:High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-184 Incomplete Blacklist

FasterXML jackson-databind before 2.8.11.1 and 2.9.x before 2.9.5 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the c3p0 libraries are available in the classpath.

- BID - 103203
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - https://github.com/FasterXML/jackson-databind/issues/1931
- CONFIRM - https://security.netapp.com/advisory/ntap-20180328-0001/
- DEBIAN - DSA-4190
- REDHAT - RHSA-2018:1447
- REDHAT - RHSA-2018:1448
- REDHAT - RHSA-2018:1449
- REDHAT - RHSA-2018:1450
- REDHAT - RHSA-2018:1451
- REDHAT - RHSA-2018:1786
- REDHAT - RHSA-2018:2088
- REDHAT - RHSA-2018:2089
- REDHAT - RHSA-2018:2090
- SECTRACK - 1040693

Vulnerable Software & Versions: (show all)

- cpe:/a:fasterxml:jackson-databind:2.3.3
- ...