



CVE-2016-3092

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2016-3092
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-04 22:59:00 UTC
Updated	2023-12-08 16:41:00 UTC
Description	The MultipartStream class in Apache Commons Fileupload before 1.3.2, as used in Apache Tomcat 7.x before 7.0.70, 8.x k

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Commons Fileupload	All	All	All	All
Application	Apache	Tomcat	7.0.0	All	All	All
Application	Apache	Tomcat	7.0.0	beta	All	All
Application	Apache	Tomcat	7.0.1	All	All	All
Application	Apache	Tomcat	7.0.10	All	All	All
Application	Apache	Tomcat	7.0.11	All	All	All
Application	Apache	Tomcat	7.0.12	All	All	All
Application	Apache	Tomcat	7.0.14	All	All	All
Application	Apache	Tomcat	7.0.16	All	All	All
Application	Apache	Tomcat	7.0.19	All	All	All
Application	Apache	Tomcat	7.0.2	All	All	All
Application	Apache	Tomcat	7.0.2	beta	All	All
Application	Apache	Tomcat	7.0.20	All	All	All
Application	Apache	Tomcat	7.0.21	All	All	All
Application	Apache	Tomcat	7.0.22	All	All	All
Application	Apache	Tomcat	7.0.23	All	All	All
Application	Apache	Tomcat	7.0.25	All	All	All

Application	Apache	Tomcat	7.0.26	All	All	All
Application	Apache	Tomcat	7.0.27	All	All	All
Application	Apache	Tomcat	7.0.28	All	All	All
Application	Apache	Tomcat	7.0.29	All	All	All
Application	Apache	Tomcat	7.0.30	All	All	All
Application	Apache	Tomcat	7.0.32	All	All	All
Application	Apache	Tomcat	7.0.33	All	All	All
Application	Apache	Tomcat	7.0.34	All	All	All
Application	Apache	Tomcat	7.0.35	All	All	All
Application	Apache	Tomcat	7.0.37	All	All	All
Application	Apache	Tomcat	7.0.39	All	All	All
Application	Apache	Tomcat	7.0.4	All	All	All
Application	Apache	Tomcat	7.0.4	beta	All	All
Application	Apache	Tomcat	7.0.40	All	All	All
Application	Apache	Tomcat	7.0.41	All	All	All
Application	Apache	Tomcat	7.0.42	All	All	All
Application	Apache	Tomcat	7.0.47	All	All	All
Application	Apache	Tomcat	7.0.5	All	All	All
Application	Apache	Tomcat	7.0.5	beta	All	All
Application	Apache	Tomcat	7.0.50	All	All	All
Application	Apache	Tomcat	7.0.52	All	All	All
Application	Apache	Tomcat	7.0.53	All	All	All
Application	Apache	Tomcat	7.0.54	All	All	All
Application	Apache	Tomcat	7.0.55	All	All	All
Application	Apache	Tomcat	7.0.56	All	All	All
Application	Apache	Tomcat	7.0.57	All	All	All
Application	Apache	Tomcat	7.0.59	All	All	All
Application	Apache	Tomcat	7.0.6	All	All	All
Application	Apache	Tomcat	7.0.61	All	All	All
Application	Apache	Tomcat	7.0.62	All	All	All
Application	Apache	Tomcat	7.0.63	All	All	All
Application	Apache	Tomcat	7.0.64	All	All	All
Application	Apache	Tomcat	7.0.65	All	All	All
Application	Apache	Tomcat	7.0.67	All	All	All
Application	Apache	Tomcat	7.0.68	All	All	All

Application	Apache	Tomcat	9.0.0	milestone1	All	All
Application	Apache	Tomcat	9.0.0	milestone3	All	All
Application	Apache	Tomcat	9.0.0	milestone4	All	All
Application	Apache	Tomcat	9.0.0	milestone6	All	All
Application	Apache	Tomcat	7.0.0	All	All	All
Application	Apache	Tomcat	7.0.0	beta	All	All
Application	Apache	Tomcat	7.0.1	All	All	All
Application	Apache	Tomcat	7.0.10	All	All	All
Application	Apache	Tomcat	7.0.11	All	All	All
Application	Apache	Tomcat	7.0.12	All	All	All
Application	Apache	Tomcat	7.0.14	All	All	All
Application	Apache	Tomcat	7.0.16	All	All	All
Application	Apache	Tomcat	7.0.19	All	All	All
Application	Apache	Tomcat	7.0.2	All	All	All
Application	Apache	Tomcat	7.0.2	beta	All	All
Application	Apache	Tomcat	7.0.20	All	All	All
Application	Apache	Tomcat	7.0.21	All	All	All
Application	Apache	Tomcat	7.0.22	All	All	All
Application	Apache	Tomcat	7.0.23	All	All	All
Application	Apache	Tomcat	7.0.25	All	All	All
Application	Apache	Tomcat	7.0.26	All	All	All
Application	Apache	Tomcat	7.0.27	All	All	All
Application	Apache	Tomcat	7.0.28	All	All	All
Application	Apache	Tomcat	7.0.29	All	All	All
Application	Apache	Tomcat	7.0.30	All	All	All
Application	Apache	Tomcat	7.0.32	All	All	All
Application	Apache	Tomcat	7.0.33	All	All	All
Application	Apache	Tomcat	7.0.34	All	All	All
Application	Apache	Tomcat	7.0.35	All	All	All
Application	Apache	Tomcat	7.0.37	All	All	All
Application	Apache	Tomcat	7.0.39	All	All	All
Application	Apache	Tomcat	7.0.4	All	All	All
Application	Apache	Tomcat	7.0.4	beta	All	All
Application	Apache	Tomcat	7.0.40	All	All	All
Application	Apache	Tomcat	7.0.41	All	All	All
Application	Apache	Tomcat	7.0.42	All	All	All

Application	Apache	Tomcat	7.0.47	All	All	All
Application	Apache	Tomcat	7.0.5	All	All	All
Application	Apache	Tomcat	7.0.5	beta	All	All
Application	Apache	Tomcat	7.0.50	All	All	All
Application	Apache	Tomcat	7.0.52	All	All	All
Application	Apache	Tomcat	7.0.53	All	All	All
Application	Apache	Tomcat	7.0.54	All	All	All
Application	Apache	Tomcat	7.0.55	All	All	All
Application	Apache	Tomcat	7.0.56	All	All	All
Application	Apache	Tomcat	7.0.57	All	All	All
Application	Apache	Tomcat	7.0.59	All	All	All
Application	Apache	Tomcat	7.0.6	All	All	All
Application	Apache	Tomcat	7.0.61	All	All	All
Application	Apache	Tomcat	7.0.62	All	All	All
Application	Apache	Tomcat	7.0.63	All	All	All
Application	Apache	Tomcat	7.0.64	All	All	All
Application	Apache	Tomcat	7.0.65	All	All	All
Application	Apache	Tomcat	7.0.67	All	All	All
Application	Apache	Tomcat	7.0.68	All	All	All
Application	Apache	Tomcat	7.0.69	All	All	All
Application	Apache	Tomcat	7.0.8	All	All	All
Application	Apache	Tomcat	8.0.0	rc1	All	All
Application	Apache	Tomcat	8.0.0	rc10	All	All
Application	Apache	Tomcat	8.0.0	rc2	All	All
Application	Apache	Tomcat	8.0.0	rc5	All	All
Application	Apache	Tomcat	8.0.1	All	All	All
Application	Apache	Tomcat	8.0.11	All	All	All
Application	Apache	Tomcat	8.0.12	All	All	All
Application	Apache	Tomcat	8.0.14	All	All	All
Application	Apache	Tomcat	8.0.15	All	All	All
Application	Apache	Tomcat	8.0.17	All	All	All
Application	Apache	Tomcat	8.0.18	All	All	All
Application	Apache	Tomcat	8.0.20	All	All	All
Application	Apache	Tomcat	8.0.21	All	All	All
Application	Apache	Tomcat	8.0.22	All	All	All

Application	Apache	Tomcat	8.0.23	All	All	All
Application	Apache	Tomcat	8.0.24	All	All	All
Application	Apache	Tomcat	8.0.26	All	All	All
Application	Apache	Tomcat	8.0.27	All	All	All
Application	Apache	Tomcat	8.0.28	All	All	All
Application	Apache	Tomcat	8.0.29	All	All	All
Application	Apache	Tomcat	8.0.3	All	All	All
Application	Apache	Tomcat	8.0.30	All	All	All
Application	Apache	Tomcat	8.0.32	All	All	All
Application	Apache	Tomcat	8.0.33	All	All	All
Application	Apache	Tomcat	8.0.35	All	All	All
Application	Apache	Tomcat	8.0.5	All	All	All
Application	Apache	Tomcat	8.0.8	All	All	All
Application	Apache	Tomcat	8.5.0	All	All	All
Application	Apache	Tomcat	8.5.2	All	All	All
Application	Apache	Tomcat	9.0.0	m1	All	All
Application	Apache	Tomcat	9.0.0	m3	All	All
Application	Apache	Tomcat	9.0.0	m4	All	All
Application	Apache	Tomcat	9.0.0	m6	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Hp	Icewall Identity Manager	5.0	All	All	All
Application	Hp	Icewall Identity Manager	5.0	All	All	All
Application	Hp	Icewall Sso Agent Option	10.0	All	All	All
Application	Hp	Icewall Sso Agent Option	10.0	All	All	All

References

Reference

Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
[Apache-SVN] Revision 1743480
HPE Intelligent Management Center (iMC) PLAT Lets Remote Users Deny Service - SecurityTracker
Debian -- Security Information -- DSA-3611-1 libcommons-fileupload-java
[Apache-SVN] Revision 1743722
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
JVN#89379547: Apache Commons FileUpload vulnerable to denial-of-service (DoS)
Document Display HPE Support Center
[Apache-SVN] Revision 1743738
Red Hat Customer Portal
Debian -- Security Information -- DSA-3609-1 tomcat8
November 2017 Apache Commons FileUpload Vulnerabilities in NetApp Products NetApp Product Security
CPU July 2018
Oracle Critical Patch Update - April 2018
Pony Mail!
Apache Commons FileUpload CVE-2016-3092 Denial Of Service Vulnerability
Red Hat Customer Portal
Red Hat Customer Portal
Document Display HPE Support Center
USN-3027-1: Tomcat vulnerability Ubuntu
Red Hat Customer Portal
JVNDB-2016-000121
HPE IceWall Identity Manager and HPE IceWall SSO Password Reset Option Lets Remote Users Deny Service - SecurityTracker
USN-3024-1: Tomcat vulnerabilities Ubuntu
Pony Mail!
Red Hat Customer Portal
1349468 – (CVE-2016-3092) CVE-2016-3092 tomcat: Usage of vulnerable FileUpload package can result in denial of service
openSUSE-SU-2016:2252-1: moderate: Security update for tomcat
Red Hat Customer Portal
Debian -- Security Information -- DSA-3614-1 tomcat7

Red Hat JBoss Enterprise Application Platform Fileupload Component Lets Remote Users Consume Excessive CPU Resources on the Target

Pony Mail!

Sun GlassFish Enterprise Server Flaws Let Remote Users Access and Modify Data and Deny Service - SecurityTracker

Apache Commons FileUpload: Multiple vulnerabilities (GLSA 202107-39) — Gentoo security

CVE-2016-3092: Apache Commons Fileupload information disclosure vulnerability

Document Display | HPE Support Center

Apache Tomcat® - Apache Tomcat 7 vulnerabilities

[Apache-SVN] Revision 1743742

Apache Tomcat® - Apache Tomcat 8 vulnerabilities

Apache Tomcat: Multiple vulnerabilities (GLSA 201705-09) — Gentoo Security

Oracle Critical Patch Update Advisory - April 2020

Red Hat Customer Portal

Oracle Critical Patch Update - July 2017

Oracle Critical Patch Update - October 2017

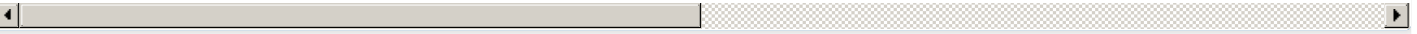
Apache Tomcat - Apache Tomcat 8 vulnerabilities

Oracle Critical Patch Update Advisory - April 2019

Oracle Solaris Bulletin - July 2016

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710049](#) Gentoo Linux Apache Commons FileUpload Multiple Vulnerabilities (GLSA 202107-39)

[753773](#) SUSE Enterprise Linux Security Update for jakarta-commons-fileupload (SUSE-SU-2023:0730-1)

[753805](#) SUSE Enterprise Linux Security Update for jakarta-commons-fileupload (SUSE-SU-2023:0758-1)

[982000](#) Java (maven) Security Update for commons-fileupload:commons-fileupload (GHSA-fvm3-cfvj-gxqq)

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)