

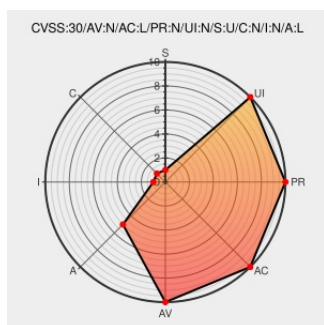


CVE-2016-3093

Published on: 06/07/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:18:00 PM UTC

CVE-2016-3093

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Struts](#) from [Apache](#) contain the following vulnerability:

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.

CVE-2016-3093 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	LOW

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Apache Struts CVE-2016-3093 Denial of Service Vulnerability	cve.report (archive) text/html	BID 90961
IBM Security Bulletin: Multiple Vulnerabilities in Struts v2 affect IBM Opportunity Detect - United States	web.archive.org text/html	CONFIRM www-01.ibm.com/support/docview.wss?

Pony Mail!

[lists.apache.org
text/html](https://lists.apache.org/text/html) MLIST [struts-dev] 20190908 Build failed in Jenkins: Struts-master-JDK8-dependency-check #204

S2-034

[Vendor Advisory
struts.apache.org
text/html](https://struts.apache.org) CONFIRM struts.apache.org/docs/s2-034.html

Apache Struts OGNL Caching Error Lets Remote Users Deny Service - SecurityTracker

[www.securitytracker.com
text/html](https://www.securitytracker.com) SECTrack 1036018

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Struts	2.0.0	All	All	All
Application	Apache	Struts	2.0.1	All	All	All
Application	Apache	Struts	2.0.10	All	All	All
Application	Apache	Struts	2.0.11	All	All	All
Application	Apache	Struts	2.0.11.1	All	All	All
Application	Apache	Struts	2.0.11.2	All	All	All
Application	Apache	Struts	2.0.12	All	All	All
Application	Apache	Struts	2.0.13	All	All	All
Application	Apache	Struts	2.0.14	All	All	All
Application	Apache	Struts	2.0.2	All	All	All
Application	Apache	Struts	2.0.3	All	All	All
Application	Apache	Struts	2.0.4	All	All	All
Application	Apache	Struts	2.0.5	All	All	All
Application	Apache	Struts	2.0.6	All	All	All
Application	Apache	Struts	2.0.7	All	All	All
Application	Apache	Struts	2.0.8	All	All	All
Application	Apache	Struts	2.0.9	All	All	All
Application	Apache	Struts	2.1.0	All	All	All
Application	Apache	Struts	2.1.1	All	All	All
Application	Apache	Struts	2.1.2	All	All	All
Application	Apache	Struts	2.1.3	All	All	All

Application	Apache	Struts	2.1.4	All	All	All
Application	Apache	Struts	2.1.5	All	All	All
Application	Apache	Struts	2.1.6	All	All	All
Application	Apache	Struts	2.1.8	All	All	All
Application	Apache	Struts	2.1.8.1	All	All	All
Application	Apache	Struts	2.2.1	All	All	All
Application	Apache	Struts	2.2.1.1	All	All	All
Application	Apache	Struts	2.2.3	All	All	All
Application	Apache	Struts	2.2.3.1	All	All	All
Application	Apache	Struts	2.3.1	All	All	All
Application	Apache	Struts	2.3.1.1	All	All	All
Application	Apache	Struts	2.3.1.2	All	All	All
Application	Apache	Struts	2.3.12	All	All	All
Application	Apache	Struts	2.3.14	All	All	All
Application	Apache	Struts	2.3.14.1	All	All	All
Application	Apache	Struts	2.3.14.2	All	All	All
Application	Apache	Struts	2.3.14.3	All	All	All
Application	Apache	Struts	2.3.15	All	All	All
Application	Apache	Struts	2.3.15.1	All	All	All
Application	Apache	Struts	2.3.15.2	All	All	All
Application	Apache	Struts	2.3.15.3	All	All	All
Application	Apache	Struts	2.3.16	All	All	All
Application	Apache	Struts	2.3.16.1	All	All	All
Application	Apache	Struts	2.3.16.2	All	All	All
Application	Apache	Struts	2.3.16.3	All	All	All
Application	Apache	Struts	2.3.20	All	All	All
Application	Apache	Struts	2.3.20.1	All	All	All
Application	Apache	Struts	2.3.20.3	All	All	All
Application	Apache	Struts	2.3.24	All	All	All
Application	Apache	Struts	2.3.24.1	All	All	All
Application	Apache	Struts	2.3.4	All	All	All
Application	Apache	Struts	2.3.4.1	All	All	All
Application	Apache	Struts	2.3.7	All	All	All
Application	Apache	Struts	2.3.8	All	All	All
Application	Apache	Struts	2.0.0	All	All	All
Application	Apache	Struts	2.0.1	All	All	All

Application	Apache	Struts	2.0.1	All	All	All
Application	Apache	Struts	2.0.10	All	All	All
Application	Apache	Struts	2.0.11	All	All	All
Application	Apache	Struts	2.0.11.1	All	All	All
Application	Apache	Struts	2.0.11.2	All	All	All
Application	Apache	Struts	2.0.12	All	All	All
Application	Apache	Struts	2.0.13	All	All	All
Application	Apache	Struts	2.0.14	All	All	All
Application	Apache	Struts	2.0.2	All	All	All
Application	Apache	Struts	2.0.3	All	All	All
Application	Apache	Struts	2.0.4	All	All	All
Application	Apache	Struts	2.0.5	All	All	All
Application	Apache	Struts	2.0.6	All	All	All
Application	Apache	Struts	2.0.7	All	All	All
Application	Apache	Struts	2.0.8	All	All	All
Application	Apache	Struts	2.0.9	All	All	All
Application	Apache	Struts	2.1.0	All	All	All
Application	Apache	Struts	2.1.1	All	All	All
Application	Apache	Struts	2.1.2	All	All	All
Application	Apache	Struts	2.1.3	All	All	All
Application	Apache	Struts	2.1.4	All	All	All
Application	Apache	Struts	2.1.5	All	All	All
Application	Apache	Struts	2.1.6	All	All	All
Application	Apache	Struts	2.1.8	All	All	All
Application	Apache	Struts	2.1.8.1	All	All	All
Application	Apache	Struts	2.2.1	All	All	All
Application	Apache	Struts	2.2.1.1	All	All	All
Application	Apache	Struts	2.2.3	All	All	All
Application	Apache	Struts	2.2.3.1	All	All	All
Application	Apache	Struts	2.3.1	All	All	All
Application	Apache	Struts	2.3.1.1	All	All	All
Application	Apache	Struts	2.3.1.2	All	All	All
Application	Apache	Struts	2.3.12	All	All	All
Application	Apache	Struts	2.3.14	All	All	All
Application	Apache	Struts	2.3.14.1	All	All	All
Application	Apache	Struts	2.3.14.2	All	All	All

Application	Apache	Struts	2.3.14.3	All	All	All
Application	Apache	Struts	2.3.15	All	All	All
Application	Apache	Struts	2.3.15.1	All	All	All
Application	Apache	Struts	2.3.15.2	All	All	All
Application	Apache	Struts	2.3.15.3	All	All	All
Application	Apache	Struts	2.3.16	All	All	All
Application	Apache	Struts	2.3.16.1	All	All	All
Application	Apache	Struts	2.3.16.2	All	All	All
Application	Apache	Struts	2.3.16.3	All	All	All
Application	Apache	Struts	2.3.20	All	All	All
Application	Apache	Struts	2.3.20.1	All	All	All
Application	Apache	Struts	2.3.20.3	All	All	All
Application	Apache	Struts	2.3.24	All	All	All
Application	Apache	Struts	2.3.24.1	All	All	All
Application	Apache	Struts	2.3.4	All	All	All
Application	Apache	Struts	2.3.4.1	All	All	All
Application	Apache	Struts	2.3.7	All	All	All
Application	Apache	Struts	2.3.8	All	All	All
Application	Ognl Project	Ognl	All	All	All	All
cpe:2.3:a:apache:struts:2.0.0:*****:						
cpe:2.3:a:apache:struts:2.0.1:*****:						
cpe:2.3:a:apache:struts:2.0.10:*****:						
cpe:2.3:a:apache:struts:2.0.11:*****:						
cpe:2.3:a:apache:struts:2.0.11.1:*****:						
cpe:2.3:a:apache:struts:2.0.11.2:*****:						
cpe:2.3:a:apache:struts:2.0.12:*****:						
cpe:2.3:a:apache:struts:2.0.13:*****:						
cpe:2.3:a:apache:struts:2.0.14:*****:						
cpe:2.3:a:apache:struts:2.0.2:*****:						
cpe:2.3:a:apache:struts:2.0.3:*****:						
cpe:2.3:a:apache:struts:2.0.4:*****:						
cpe:2.3:a:apache:struts:2.0.5:*****:						

cpe:2.3:a:apache:struts:2.0.6:*****:
cpe:2.3:a:apache:struts:2.0.7:*****:
cpe:2.3:a:apache:struts:2.0.8:*****:
cpe:2.3:a:apache:struts:2.0.9:*****:
cpe:2.3:a:apache:struts:2.1.0:*****:
cpe:2.3:a:apache:struts:2.1.1:*****:
cpe:2.3:a:apache:struts:2.1.2:*****:
cpe:2.3:a:apache:struts:2.1.3:*****:
cpe:2.3:a:apache:struts:2.1.4:*****:
cpe:2.3:a:apache:struts:2.1.5:*****:
cpe:2.3:a:apache:struts:2.1.6:*****:
cpe:2.3:a:apache:struts:2.1.8:*****:
cpe:2.3:a:apache:struts:2.1.8.1:*****:
cpe:2.3:a:apache:struts:2.2.1:*****:
cpe:2.3:a:apache:struts:2.2.1.1:*****:
cpe:2.3:a:apache:struts:2.2.3:*****:
cpe:2.3:a:apache:struts:2.2.3.1:*****:
cpe:2.3:a:apache:struts:2.3.1:*****:
cpe:2.3:a:apache:struts:2.3.1.1:*****:
cpe:2.3:a:apache:struts:2.3.1.2:*****:
cpe:2.3:a:apache:struts:2.3.12:*****:
cpe:2.3:a:apache:struts:2.3.14:*****:
cpe:2.3:a:apache:struts:2.3.14.1:*****:
cpe:2.3:a:apache:struts:2.3.14.2:*****:
cpe:2.3:a:apache:struts:2.3.14.3:*****:
cpe:2.3:a:apache:struts:2.3.15:*****:
cpe:2.3:a:apache:struts:2.3.15.1:*****:
cpe:2.3:a:apache:struts:2.3.15.2:*****:

cpe:2.3:a:apache:struts:2.3.15.3:*****:
cpe:2.3:a:apache:struts:2.3.16:*****:
cpe:2.3:a:apache:struts:2.3.16.1:*****:
cpe:2.3:a:apache:struts:2.3.16.2:*****:
cpe:2.3:a:apache:struts:2.3.16.3:*****:
cpe:2.3:a:apache:struts:2.3.20:*****:
cpe:2.3:a:apache:struts:2.3.20.1:*****:
cpe:2.3:a:apache:struts:2.3.20.3:*****:
cpe:2.3:a:apache:struts:2.3.24:*****:
cpe:2.3:a:apache:struts:2.3.24.1:*****:
cpe:2.3:a:apache:struts:2.3.4:*****:
cpe:2.3:a:apache:struts:2.3.4.1:*****:
cpe:2.3:a:apache:struts:2.3.7:*****:
cpe:2.3:a:apache:struts:2.3.8:*****:
cpe:2.3:a:apache:struts:2.0.0:*****:
cpe:2.3:a:apache:struts:2.0.1:*****:
cpe:2.3:a:apache:struts:2.0.10:*****:
cpe:2.3:a:apache:struts:2.0.11:*****:
cpe:2.3:a:apache:struts:2.0.11.1:*****:
cpe:2.3:a:apache:struts:2.0.11.2:*****:
cpe:2.3:a:apache:struts:2.0.12:*****:
cpe:2.3:a:apache:struts:2.0.13:*****:
cpe:2.3:a:apache:struts:2.0.14:*****:
cpe:2.3:a:apache:struts:2.0.2:*****:
cpe:2.3:a:apache:struts:2.0.3:*****:
cpe:2.3:a:apache:struts:2.0.4:*****:
cpe:2.3:a:apache:struts:2.0.5:*****:
cpe:2.3:a:apache:struts:2.0.6:*****:
cpe:2.3:a:apache:struts:2.0.7:*****:

cpe:2.3:a:apache:struts:2.0.8:*****:
cpe:2.3:a:apache:struts:2.0.9:*****:
cpe:2.3:a:apache:struts:2.1.0:*****:
cpe:2.3:a:apache:struts:2.1.1:*****:
cpe:2.3:a:apache:struts:2.1.2:*****:
cpe:2.3:a:apache:struts:2.1.3:*****:
cpe:2.3:a:apache:struts:2.1.4:*****:
cpe:2.3:a:apache:struts:2.1.5:*****:
cpe:2.3:a:apache:struts:2.1.6:*****:
cpe:2.3:a:apache:struts:2.1.8:*****:
cpe:2.3:a:apache:struts:2.1.8.1:*****:
cpe:2.3:a:apache:struts:2.2.1:*****:
cpe:2.3:a:apache:struts:2.2.1.1:*****:
cpe:2.3:a:apache:struts:2.2.3:*****:
cpe:2.3:a:apache:struts:2.2.3.1:*****:
cpe:2.3:a:apache:struts:2.3.1:*****:
cpe:2.3:a:apache:struts:2.3.1.1:*****:
cpe:2.3:a:apache:struts:2.3.1.2:*****:
cpe:2.3:a:apache:struts:2.3.12:*****:
cpe:2.3:a:apache:struts:2.3.14:*****:
cpe:2.3:a:apache:struts:2.3.14.1:*****:
cpe:2.3:a:apache:struts:2.3.14.2:*****:
cpe:2.3:a:apache:struts:2.3.14.3:*****:
cpe:2.3:a:apache:struts:2.3.15:*****:
cpe:2.3:a:apache:struts:2.3.15.1:*****:
cpe:2.3:a:apache:struts:2.3.15.2:*****:
cpe:2.3:a:apache:struts:2.3.15.3:*****:
cpe:2.3:a:apache:struts:2.3.16:*****:

cpe:2.3:a:apache:struts:2.3.16.1:*****:
cpe:2.3:a:apache:struts:2.3.16.2:*****:
cpe:2.3:a:apache:struts:2.3.16.3:*****:
cpe:2.3:a:apache:struts:2.3.20:*****:
cpe:2.3:a:apache:struts:2.3.20.1:*****:
cpe:2.3:a:apache:struts:2.3.20.3:*****:
cpe:2.3:a:apache:struts:2.3.24:*****:
cpe:2.3:a:apache:struts:2.3.24.1:*****:
cpe:2.3:a:apache:struts:2.3.4:*****:
cpe:2.3:a:apache:struts:2.3.4.1:*****:
cpe:2.3:a:apache:struts:2.3.7:*****:
cpe:2.3:a:apache:struts:2.3.8:*****:
cpe:2.3:a:ognl_project:ognl:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)