

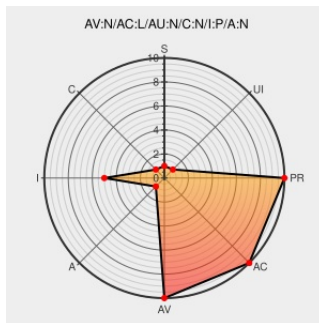


CVE-2011-5057

Published on: 01/08/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:17 PM UTC

CVE-2011-5057

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

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

Apache Struts 2.3.1.2 and earlier, 2.3.19-2.3.23, provides interfaces that do not properly restrict access to collections such as the session and request collections, which might allow remote attackers to modify run-time data values via a crafted parameter to an application that implements an affected interface, as demonstrated by the

SessionAware, RequestAware, ApplicationAware, ServletRequestAware, ServletResponseAware, and ParameterAware interfaces. NOTE: the vendor disputes the significance of this report because of an "easy work-around in existing apps by configuring the interceptor."

CVE-2011-5057 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

[WW-3631] Implementing SessionAware allows session tampering - ASF JIRA

[Issue Tracking](#)
[Vendor Advisory](#)
[issues.apache.org](#)
[text/html](#)

[CONFIRM](#)
[issues.apache.org/jira/browse/WW-3631](#)

Security Advisory SA47109 - Struts2 SessionAware / RequestAware Session Manipulation Weakness - Secunia

[Permissions Required](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 47109](#)

Code Secure: Struts 2 Session Tampering via
SessionAware/RequestAware WW-3631

Third Party Advisory

codesecure.blogspot.com

text/html

MISC

codesecure.blogspot.com/2011/12/struts-2-session-tampering-via.html

[WW-2264] A session value is overwritten by requesting. - ASF JIRA

Issue Tracking

Vendor Advisory

issues.apache.org

text/html

CONFIRM

issues.apache.org/jira/browse/WW-2264

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	All	All	All	All
Application	Apache	Struts	All	All	All	All
cpe:2.3:a:apache:struts:*****:						
cpe:2.3:a:apache:struts:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)