



CVE-2012-1592

Published on: 12/05/2019 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:24:00 AM UTC

CVE-2012-1592

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

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

A local code execution issue exists in Apache Struts2 when processing malformed XSLT files, which could let a malicious user upload and execute arbitrary files.

CVE-2012-1592 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **libstruts1.2-java** - **libstruts1.2-java** version = 1.2-

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
oss-security - Re: CVE request: Struts2 xsltResult local code execution flaw	Mailing List Third Party Advisory www.openwall.com	www.openwall.com/lists/oss-security/2012/03/28/12

	www.pentestlab.com text/html	
Pony Mail!	lists.apache.org text/html	MLIST [struts-issues] 20200122 [jira] [Created] (WW-5055) Fix for security vulnerability CVE-2012-1592 identified in the National Vulnerability Database
807485 – (CVE-2012-1592) CVE-2012-1592 struts2: xsltResult local code execution flaw	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=CVE-2012-1592
Pony Mail!	lists.apache.org text/html	MLIST [struts-issues] 20200903 [jira] [Commented] (WW-5055) Fix for security vulnerability CVE-2012-1592 identified in the National Vulnerability Database
CVE-2012-1592	Third Party Advisory security-tracker.debian.org text/html	MISC security-tracker.debian.org/tracker/CVE-2012-1592
Pony Mail!	lists.apache.org text/html	MLIST [struts-issues] 20200123 [jira] [Closed] (WW-5055) Fix for security vulnerability CVE-2012-1592 identified in the National Vulnerability Database
CVE-2012-1592 - Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	MISC access.redhat.com/security/cve/cve-2012-1592

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	2.0.0	All	All	All
cpe:2.3:a:apache:struts:2.0.0:*****:						
cpe:2.3:a:apache:struts:2.0.0:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/digitalmunition	Apache Struts XSLT File Code Execution [CVE-2012-1592] https://t.co/Y5eZ4GFFLr	2019-12-08 11:44:22

[← 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](#)