



Published on: 11/22/2005 12:00:00 AM UTC

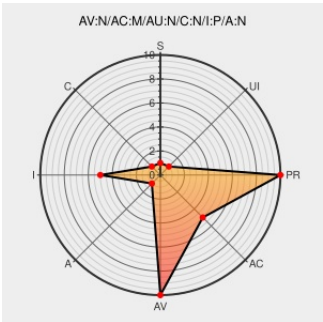
Last Modified on: 03/23/2021 11:27:23 PM UTC

CVE-2005-3745

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

Cross-site scripting (XSS) vulnerability in Apache Struts 1.2.7, and possibly other versions allows remote attackers to inject arbitrary web script or HTML via the query string, which is not properly quoted or filtered when the request handler generates an error message.

CVE-2005-3745 has been assigned by  cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Secunia - Advisories - Struts Error Message Cross-Site Scripting Vulnerability	web.archive.org text/html	 SECUNIA 17677
Pony Mail!	lists.apache.org text/html	 MLIST [struts-issues] 20201207 [jira] [Created] (WW-5105) Tracking the fix commit of CVE-2005-3745 and CVE-2018-1327
Red Hat Application Server Struts Error Message Cross-Site Scripting - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	 SECUNIA 18341
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	 VUPEN ADV-2005-2525
Apache Struts Error Response Cross-Site Scripting Vulnerability	Exploit Patch cve.report (archive)	 BID 15512

	text/html	
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051121 Security Advisory: Struts Error Message Cross Site Scripting
Support	www.redhat.com text/html	REDHAT RHSA-2006:0157
rhn.redhat.com Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2006:0161
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 21021
SecurityTracker.com Archives - Struts Input Validation Hole in Error Message Permits Cross-Site Scripting Attacks	securitytracker.com text/html	SECTrack 1015257
Pony Mail!	lists.apache.org text/html	MLIST [struts-issues] 20201207 [jira] [Updated] (WW-5105) Tracking the fix commit of CVE-2005-3745 and CVE-2018-1327
Hacktics - Application Security Experts - Publications	Exploit Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.hacktics.com/AdvStrutsNov05.html
Struts Error Message Cross Site Scripting - CXSecurity.com	securityreason.com text/html	SREASON 197

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.

Related QID Numbers

995388 Java (Maven) Security Update for org.apache.struts:struts-core (GHSA-9cjh-qmvx-436c)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Struts	1.2.7	All	All	All
Application	Apache	Struts	1.2.7	All	All	All
cpe:2.3:a:apache:struts:1.2.7:*****:						
cpe:2.3:a:apache:struts:1.2.7:*****:						

No vendor comments have been submitted for this CVE

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](#)