



CVE-2008-6504

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

Summary

CVE	CVE-2008-6504
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-23 14:19:00 UTC
Updated	2017-08-17 01:29:00 UTC
Description	ParametersInterceptor in OpenSymphony XWork 2.0.x before 2.0.6 and 2.1.x before 2.1.2, as used in Apache Struts and o

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Struts	2.0.0	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	2.0.2	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	2.0.0	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	2.0.2	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	Opensymphony	Xwork	2.0.0	All	All	All
Application	Opensymphony	Xwork	2.0.1	All	All	All
Application	Opensymphony	Xwork	2.0.2	All	All	All
Application	Opensymphony	Xwork	2.0.3	All	All	All
Application	Opensymphony	Xwork	2.0.4	All	All	All
Application	Opensymphony	Xwork	2.0.5	All	All	All
Application	Opensymphony	Xwork	2.1.0	All	All	All
Application	Opensymphony	Xwork	2.1.1	All	All	All
Application	Opensymphony	Xwork	2.0.0	All	All	All
Application	Opensymphony	Xwork	2.0.1	All	All	All
Application	Opensymphony	Xwork	2.0.2	All	All	All
Application	Opensymphony	Xwork	2.0.3	All	All	All
Application	Opensymphony	Xwork	2.0.4	All	All	All
Application	Opensymphony	Xwork	2.0.5	All	All	All
Application	Opensymphony	Xwork	2.1.0	All	All	All
Application	Opensymphony	Xwork	2.1.1	All	All	All

References						
Reference					Source	Link
XWork 'ParameterInterceptor' Class OGNL Security Bypass Vulnerability					BID	www.bids
[#XW-641] XWork ParameterInterceptors bypass (OGNL statement execution) - OpenSymphony JIRA					CONFIRM	jira.opensymphony.org
49732					OSVDB	osvdb.org
S2-003					CONFIRM	struts.apache.org
Apache Struts Security Bypass and Directory Traversal - Secunia Advisories - Vulnerability Intelligence - Secunia.com					SECUNIA	secunia.com
IBM X-Force Exchange					XF	exchange.xforce.ibmcloud.com
XWork "ParameterInterceptor" Security Bypass Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com					SECUNIA	secunia.com
404 Not Found					CONFIRM	issues.apache.org
CR-9 OAK-484 QueryResultTest failing - Abandoned					CONFIRM	fisher.apache.org
XWork "ParameterInterceptor" Security Bypass Vulnerability - Vulnerability Intelligence - Secunia.com					VULNERABILITY INTELLIGENCE	secunia.com

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	wv
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	wv
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

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