



CVE-2007-4556

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

Summary

CVE	CVE-2007-4556
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-08-28 01:17:00 UTC
Updated	2018-10-26 14:00:00 UTC
Description	Struts support in OpenSymphony XWork before 1.2.3, and 2.x before 2.0.4, as used in WebWork and Apache Struts, recur

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opensymphony	Xwork	All	All	All	All
Application	Opensymphony	Xwork	All	All	All	All
Application	Opensymphony	Xwork	All	All	All	All

References

Reference	Source	Link
S2-001	CONFIRM	struts.apache.org
Opensymphony WebWork XWork Input Validation OGNL Command Injection - Advisories - Secunia	SECUNIA	secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
[#XW-544] User input is evaluated as an OGNL expression - OpenSymphony JIRA	CONFIRM	jira.opensymphony.com
37072	OSVDB	osvdb.org
[#WW-2030] User input is evaluated as an OGNL expression - Apache Struts JIRA	CONFIRM	issues.apache.org
XWork Input Validation OGNL Command Injection Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Release Notes - XWork - Version 1.2.3 - HTML format - OpenSymphony JIRA	CONFIRM	jira.opensymphony.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
OpenSymphony Support Forums: XWork 1.2.3 Security Update released	CONFIRM	forums.opensymphony.com
Release Notes - XWork - Version 2.0.4 - HTML format - OpenSymphony JIRA	CONFIRM	jira.opensymphony.com

1.2.3 Press Release - WebWork - Confluence	CONFIRM	wiki.opensymphony.com
XWork AltSyntax OGNL Input Validation Vulnerability	BID	www.securityfocus.com
Apache Struts XWork Input Validation OGNL Command Injection Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report