



# CVE-2006-1547

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

## Summary

<b>CVE</b>	CVE-2006-1547
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-03-30 22:02:00 UTC
<b>Updated</b>	2026-04-16 14:02:43 UTC
<b>Description</b>	ActionForm in Apache Software Foundation (ASF) Struts before 1.2.9 with BeanUtils 1.7 allows remote attackers to cause a

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**EPSS:** 0.221920000 probability, percentile 0.958230000 (date 2026-04-22)

**CISA KEV:** Listed on 2022-01-21; due 2022-07-21; ransomware use Unknown

**Problem Types:** NVD-CWE-Other | CWE-749 | n/a | CWE-749 CWE-749 Exposed Dangerous Method or Function

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	7.8		AV:N/AC:L/Au:N/C:N/I:N/A:C

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:N/AC:L/Au:N/C:N/I:N/A:C

### CISA Known Exploited Vulnerability

<b>Vendor</b>	Apache
<b>Product</b>	Struts 1
<b>Name</b>	Apache Struts 1 ActionForm Denial-of-Service Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2006-1547">https://nvd.nist.gov/vuln/detail/CVE-2006-1547</a>

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Commons Beanutils</a>	1.7.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Struts</a>	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Na</a>	<a href="#">N/a</a>	affected n/a	Not specified

## References

Reference
Struts Multiple Vulnerabilities - Advisories - Secunia
Missing Bug ID
SecurityTracker.com Archives - Struts Bugs May Let Remote Users Bypass Validation, Conduct Cross-Site Scripting Attacks, and Deny Service
SUSE Updates for Multiple Packages - Advisories - Secunia
SUSE Security announcements: [suse-security-announce] SUSE Security Summary Report SUSE-SR:2006:010
Struts Release Notes (since 1.2.8)
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
www.cisa.gov/known-exploited-vulnerabilities-catalog
IBM X-Force Exchange
Apache Struts Multiple Remote Vulnerabilities
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

Source	Time	Event
ADP	2022-01-21T00:00:00.000Z	CVE-2006-1547 added to CISA KEV

## Legacy QID Mappings

376432 Apache Struts Denial of Service (DoS) Vulnerability

© 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](#)