



CVE-2006-1546

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2006-1546
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-03-30 22:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Apache Software Foundation (ASF) Struts before 1.2.9 allows remote attackers to bypass validation via a request with a 'or

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

EPSS: 0.016120000 probability, percentile 0.818000000 (date 2026-04-19)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Apache	Struts	All	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference						
Struts Multiple Vulnerabilities - Advisories - Secunia						
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						
Missing Bug ID						
Mailing list archives						
Re: Validation Security Hole?						
IBM X-Force Exchange						
Apache Struts Multiple Remote Vulnerabilities						
Re: Validation Security Hole?						
Mailing list archives						
CVE Program record						
NVD vulnerability detail						
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						