

CVE-2013-2251

Apache Struts Improper Input Validation Vulnerability

Exigent

CISA KEV since Mar 25, 2022

Actively exploited

Public exploit module (Metasploit)

Apache Struts 2.0.0 through 2.3.15 allows remote attackers to execute arbitrary OGNL expressions via a parameter with a crafted (1) action:, (2) redirect:, or (3) redirectAction: prefix.

EVRS

87/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.999

99.99th percentile · FIRST

CISA DEADLINE

Apr 15, 2022

KEV since 2022 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 1 more affected product on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.apache.struts:struts2-core	< 2.3.15.1	2.3.15.1	GitHub
archiva	≥ 1.3 < 1.3.8 1.2 1.2.2	1.3.8	NVD
struts	≥ 2.0.0 ≤ 2.3.15	after 2.3.15	NVD
interstage business process manager analytics	12.0 12.1	no fixed version listed	NVD
siebel apps - e-billing	6.1 6.1.1 6.2	no fixed version listed	NVD
windows server 2003	—	no fixed version listed	NVD
windows server 2008	—	no fixed version listed	NVD
enterprise linux	≥ 5.0 ≤ 6.10	no fixed version listed	NVD
windows server 2012	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-47qp-8v9g-39hp**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**Current data** evulnable.com/vulnerability-management/cve/CVE-2013-2251**NVD** nvd.nist.gov/vuln/detail/CVE-2013-2251**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2022-2328

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.