

CVE-2012-0391

Apache Struts 2 Improper Input Validation Vulnerability

CISA KEV since Jan 21, 2022

Actively exploited

Public exploit module (Metasploit)

The ExceptionDelegator component in Apache Struts before 2.2.3.1 interprets parameter values as OGNL expressions during certain exception handling for mismatched data types of properties, which allows remote attackers to execute arbitrary Java code via a crafted parameter.

EVRS 81/100 Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.756 99.52nd percentile · FIRST	CISA DEADLINE Jul 21, 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	0.756 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.apache.struts:struts2-core	< 2.2.3.1	2.2.3.1	GitHub
org.apache.struts.xwork:xwork-core	< 2.2.3.1	2.2.3.1	GitHub
struts	< 2.2.3.1	2.2.3.1	NVD

Sources

Vendor guidance github.com/advisories/GHSA-4wrr-9h5r-m92w
NVD nvd.nist.gov/vuln/detail/CVE-2012-0391

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-2464

Additional guidance issues.apache.org/jira/browse/WW-3668
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2012-0391

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