CVE-2012-0391

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

Summary

CVE	CVE-2012-0391
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-01-08 15:55:01 UTC
Updated	2026-04-22 10:36:05 UTC
Description	The ExceptionDelegator component in Apache Struts before 2.2.3.1 interprets parameter values as OGNL expressions duri

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.883190000 probability, percentile 0.994990000 (date 2026-04-21)

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

Problem Types: CWE-94 | n/a | CWE-94 CWE-94 Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9.3		AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

CISA Known Exploited Vulnerability

Vendor	Apache
Product	Struts 2
Name	Apache Struts 2 Improper Input Validation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2012-0391

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	Source
NEOHAPSIS - Peace of Mind Through Integrity and Insight	af854a3a-2127-422
Version Notes 2.3.11 - Apache Struts 2 Wiki - Apache Software Foundation	af854a3a-2127-422
404 - Page not found! - SEC Consult	af854a3a-2127-422
Apache Struts2 <= 2.3.1 Multiple Vulnerabilities	af854a3a-2127-422
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2
[#WW-3668] Vulnerability: User input is evaluated as an OGNL expression when there's a conversion error. - ASF JIRA	af854a3a-2127-422
S2-008 - Apache Struts 2 Wiki - Apache Software Foundation	af854a3a-2127-422
About Secunia Research | Flexera	af854a3a-2127-422
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-01-21T00:00:00.000Z	CVE-2012-0391 added to CISA KEV

Legacy QID Mappings

995344 Java (Maven) Security Update for org.apache.struts:struts2-parent (GHSA-4wrr-9h5r-m92w)