CVE-2013-2251

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

Summary

CVE	CVE-2013-2251
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-07-20 03:37:00 UTC
Updated	2020-10-20 22:15:00 UTC
Description	Apache Struts 2.0.0 through 2.3.15 allows remote attackers to execute arbitrary OGNL expressions via a parameter with a

Risk And Classification

EPSS: 0.943250000 probability, percentile 0.999520000 (date 2026-04-16)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Unknown

Problem Types: CWE-20

CISA Known Exploited Vulnerability

Vendor	Apache
Product	Struts
Name	Apache Struts Improper Input Validation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2013-2251

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Struts	2.0.0	All	All	All
Application	Apache	Struts	2.0.1	All	All	All
Application	Apache	Struts	2.0.10	All	All	All
Application	Apache	Struts	2.0.11	All	All	All
Application	Apache	Struts	2.0.11.1	All	All	All
Application	Apache	Struts	2.0.11.2	All	All	All
Application	Apache	Struts	2.0.12	All	All	All
Application	Apache	Struts	2.0.13	All	All	All

Application	Apache	Struts	2.0.14	All	All	All
Application	Apache	Struts	2.0.2	All	All	All
Application	Apache	Struts	2.0.3	All	All	All
Application	Apache	Struts	2.0.4	All	All	All
Application	Apache	Struts	2.0.5	All	All	All
Application	Apache	Struts	2.0.6	All	All	All
Application	Apache	Struts	2.0.7	All	All	All
Application	Apache	Struts	2.0.8	All	All	All
Application	Apache	Struts	2.0.9	All	All	All
Application	Apache	Struts	2.1.0	All	All	All
Application	Apache	Struts	2.1.1	All	All	All
Application	Apache	Struts	2.1.2	All	All	All
Application	Apache	Struts	2.1.3	All	All	All
Application	Apache	Struts	2.1.4	All	All	All
Application	Apache	Struts	2.1.5	All	All	All
Application	Apache	Struts	2.1.6	All	All	All
Application	Apache	Struts	2.1.8	All	All	All
Application	Apache	Struts	2.1.8.1	All	All	All
Application	Apache	Struts	2.2.1	All	All	All
Application	Apache	Struts	2.2.1.1	All	All	All
Application	Apache	Struts	2.2.3	All	All	All
Application	Apache	Struts	2.2.3.1	All	All	All
Application	Apache	Struts	2.3.1	All	All	All
Application	Apache	Struts	2.3.1.1	All	All	All
Application	Apache	Struts	2.3.1.2	All	All	All
Application	Apache	Struts	2.3.12	All	All	All
Application	Apache	Struts	2.3.14	All	All	All
Application	Apache	Struts	2.3.14.1	All	All	All
Application	Apache	Struts	2.3.14.2	All	All	All
Application	Apache	Struts	2.3.14.3	All	All	All
Application	Apache	Struts	2.3.15	All	All	All
Application	Apache	Struts	2.3.3	All	All	All
Application	Apache	Struts	2.3.4	All	All	All
Application	Apache	Struts	2.3.4.1	All	All	All
Application	Apache	Struts	2.3.7	All	All	All

Application	Apache	Struts	2.3.8	All	All	All
Application	Apache	Struts	2.0.0	All	All	All
Application	Apache	Struts	2.0.1	All	All	All
Application	Apache	Struts	2.0.10	All	All	All
Application	Apache	Struts	2.0.11	All	All	All
Application	Apache	Struts	2.0.11.1	All	All	All
Application	Apache	Struts	2.0.11.2	All	All	All
Application	Apache	Struts	2.0.12	All	All	All
Application	Apache	Struts	2.0.13	All	All	All
Application	Apache	Struts	2.0.14	All	All	All
Application	Apache	Struts	2.0.2	All	All	All
Application	Apache	Struts	2.0.3	All	All	All
Application	Apache	Struts	2.0.4	All	All	All
Application	Apache	Struts	2.0.5	All	All	All
Application	Apache	Struts	2.0.6	All	All	All
Application	Apache	Struts	2.0.7	All	All	All
Application	Apache	Struts	2.0.8	All	All	All
Application	Apache	Struts	2.0.9	All	All	All
Application	Apache	Struts	2.1.0	All	All	All
Application	Apache	Struts	2.1.1	All	All	All
Application	Apache	Struts	2.1.2	All	All	All
Application	Apache	Struts	2.1.3	All	All	All
Application	Apache	Struts	2.1.4	All	All	All
Application	Apache	Struts	2.1.5	All	All	All
Application	Apache	Struts	2.1.6	All	All	All
Application	Apache	Struts	2.1.8	All	All	All
Application	Apache	Struts	2.1.8.1	All	All	All
Application	Apache	Struts	2.2.1	All	All	All
Application	Apache	Struts	2.2.1.1	All	All	All
Application	Apache	Struts	2.2.3	All	All	All
Application	Apache	Struts	2.2.3.1	All	All	All
Application	Apache	Struts	2.3.1	All	All	All
Application	Apache	Struts	2.3.1.1	All	All	All
Application	Apache	Struts	2.3.1.2	All	All	All
Application	Apache	Struts	2.3.12	All	All	All

Application	Apache	Struts	2.3.14	All	All	All
Application	Apache	Struts	2.3.14.1	All	All	All
Application	Apache	Struts	2.3.14.2	All	All	All
Application	Apache	Struts	2.3.14.3	All	All	All
Application	Apache	Struts	2.3.15	All	All	All
Application	Apache	Struts	2.3.3	All	All	All
Application	Apache	Struts	2.3.4	All	All	All
Application	Apache	Struts	2.3.4.1	All	All	All
Application	Apache	Struts	2.3.7	All	All	All
Application	Apache	Struts	2.3.8	All	All	All

References

Reference
Archiva - Security Vulnerabilities
This page provides Security Information. - Fujitsu Global
Oracle Critical Patch Update - July 2015
Apache Archiva 1.3.6 => Remote Command Execution 0day - CXSecurity.com
Oracle Critical Patch Update - January 2014
Full Disclosure: Apache Software Foundation A Subsite Remote command execution
oss-sec: Re: CVE Request: Apache Archiva Remote Command Execution 0day
Oracle Siebel Enterprise Flaws Let Remote Users Partially Access and Modify Data and Gain Elevated Privileges - SecurityTracker
IBM X-Force Exchange
RETIRED: Oracle January 2014 Critical Patch Update Multiple Vulnerabilities
Cisco Security Advisory: Apache Struts 2 Command Execution Vulnerability in Multiple Cisco Products
98445
Apache Struts CVE-2013-2251 Multiple Remote Command Execution Vulnerabilities
S2-016
MySQL Multiple Bugs Let Remote Authenticated Users Execute Arbitrary Code, Deny Service, and Partially Access and Modify Data - Securit
Apache Struts 2 Remote Code Execution ≈ Packet Storm
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.