



CVE-2017-9805

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-9805
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-15 19:29:00 UTC
Updated	2019-08-12 21:15:00 UTC
Description	The REST Plugin in Apache Struts 2.1.1 through 2.3.x before 2.3.34 and 2.5.x before 2.5.13 uses an XStreamHandler with

Risk And Classification

EPSS: 0.943220000 probability, percentile 0.999510000 (date 2026-04-07)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-502

CISA Known Exploited Vulnerability

Vendor	Apache
Product	Struts
Name	Apache Struts Deserialization of Untrusted Data Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-9805

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	2.3.15.1	All	All	All
Application	Apache	Struts	2.3.15.2	All	All	All
Application	Apache	Struts	2.3.15.3	All	All	All
Application	Apache	Struts	2.3.16	All	All	All
Application	Apache	Struts	2.3.16.1	All	All	All
Application	Apache	Struts	2.3.16.2	All	All	All
Application	Apache	Struts	2.3.16.3	All	All	All
Application	Apache	Struts	2.3.20	All	All	All
Application	Apache	Struts	2.3.20.1	All	All	All
Application	Apache	Struts	2.3.20.3	All	All	All
Application	Apache	Struts	2.3.24	All	All	All
Application	Apache	Struts	2.3.24.1	All	All	All
Application	Apache	Struts	2.3.24.3	All	All	All
Application	Apache	Struts	2.3.28	All	All	All
Application	Apache	Struts	2.3.28.1	All	All	All
Application	Apache	Struts	2.3.29	All	All	All
Application	Apache	Struts	2.3.3	All	All	All
Application	Apache	Struts	2.3.30	All	All	All
Application	Apache	Struts	2.3.31	All	All	All
Application	Apache	Struts	2.3.32	All	All	All
Application	Apache	Struts	2.3.33	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	2.5.1	All	All	All
Application	Apache	Struts	2.5.10	All	All	All
Application	Apache	Struts	2.5.10.1	All	All	All
Application	Apache	Struts	2.5.11	All	All	All
Application	Apache	Struts	2.5.12	All	All	All
Application	Apache	Struts	2.5.2	All	All	All
Application	Apache	Struts	2.5.3	All	All	All
Application	Apache	Struts	2.5.4	All	All	All
Application	Apache	Struts	2.5.5	All	All	All
Application	Apache	Struts	2.5.6	All	All	All
Application	Apache	Struts	2.5.7	All	All	All
Application	Apache	Struts	2.5.8	All	All	All
Application	Apache	Struts	2.5.9	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	2.3.15.1	All	All	All
Application	Apache	Struts	2.3.15.2	All	All	All
Application	Apache	Struts	2.3.15.3	All	All	All
Application	Apache	Struts	2.3.16	All	All	All
Application	Apache	Struts	2.3.16.1	All	All	All
Application	Apache	Struts	2.3.16.2	All	All	All
Application	Apache	Struts	2.3.16.3	All	All	All
Application	Apache	Struts	2.3.20	All	All	All
Application	Apache	Struts	2.3.20.1	All	All	All
Application	Apache	Struts	2.3.20.3	All	All	All
Application	Apache	Struts	2.3.24	All	All	All
Application	Apache	Struts	2.3.24.1	All	All	All
Application	Apache	Struts	2.3.24.3	All	All	All
Application	Apache	Struts	2.3.28	All	All	All
Application	Apache	Struts	2.3.28.1	All	All	All
Application	Apache	Struts	2.3.29	All	All	All
Application	Apache	Struts	2.3.3	All	All	All
Application	Apache	Struts	2.3.30	All	All	All
Application	Apache	Struts	2.3.31	All	All	All
Application	Apache	Struts	2.3.32	All	All	All
Application	Apache	Struts	2.3.33	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	2.5.1	All	All	All
Application	Apache	Struts	2.5.10	All	All	All
Application	Apache	Struts	2.5.10.1	All	All	All
Application	Apache	Struts	2.5.11	All	All	All
Application	Apache	Struts	2.5.12	All	All	All
Application	Apache	Struts	2.5.2	All	All	All
Application	Apache	Struts	2.5.3	All	All	All
Application	Apache	Struts	2.5.4	All	All	All
Application	Apache	Struts	2.5.5	All	All	All
Application	Apache	Struts	2.5.6	All	All	All
Application	Apache	Struts	2.5.7	All	All	All

Application	Apache	Struts	2.5.8	All	All	All
Application	Apache	Struts	2.5.9	All	All	All
References						
Reference						
CVE-2017-9805 Apache Struts Vulnerability in Multiple NetApp Products NetApp Product Security						
S2-052 - Apache Struts 2 Documentation - Apache Software Foundation						
Using QL to find a remote code execution vulnerability in Apache Struts (CVE-2017-9805) - Blog - lgtm						
Vulnerability Note VU#112992 - Apache Struts 2 framework REST plugin insecurely deserializes untrusted XML data						
Apache Struts 2.5 < 2.5.12 - REST Plugin XStream Remote Code Execution						
Oracle Security Alert CVE-2017-9805						
S2-052 - Apache Struts 2 Documentation - Apache Software Foundation						
Apache Struts Statement on Equifax Security Breach : The Apache Software Foundation Blog						
Apache Struts CVE-2017-9805 Remote Code Execution Vulnerability						
Apache Struts REST Plugin XStream Deserialization Flaw Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker						
Bug 1488482 – CVE-2017-9805 struts: RCE attack via REST plugin with XStream handler to deserialise XML requests						
Multiple Vulnerabilities in Apache Struts 2 Affecting Cisco Products: September 2017						
CVE Program record						
NVD vulnerability detail						
CISA Known Exploited Vulnerabilities catalog						
No vendor comments have been submitted for this CVE.						
Legacy QID Mappings						
981081 Java (maven) Security Update for org.apache.struts:struts2-rest-plugin (GHSA-gg9m-fj3v-r58c)						

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)