



CVE-2020-17530

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

Summary

CVE	CVE-2020-17530
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-11 02:15:00 UTC
Updated	2022-06-03 16:38:00 UTC
Description	Forced OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution. Affected

Risk And Classification

EPSS: 0.943760000 probability, percentile 0.999670000 (date 2026-04-01)

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

Problem Types: CWE-917

CISA Known Exploited Vulnerability

Vendor	Apache
Product	Struts
Name	Apache Struts Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-17530

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Struts	All	All	All	All
Application	Apache	Struts	All	All	All	All
Application	Oracle	Business Intelligence	12.2.1.3.0	All	All	All
Application	Oracle	Business Intelligence	12.2.1.4.0	All	All	All
Application	Oracle	Communications Diameter Intelligence Hub	8.0.0	All	All	All
Application	Oracle	Communications Diameter Intelligence Hub	8.1.0	All	All	All
Application	Oracle	Communications Diameter Intelligence Hub	8.2.0	All	All	All
Application	Oracle	Communications Diameter Intelligence Hub	8.2.3	All	All	All

Application	Oracle	Communications Policy Management	12.5.0	All	All	All
Application	Oracle	Communications Pricing Design Center	12.0.0.3.0	All	All	All
Application	Oracle	Financial Services Data Integration Hub	8.0.3	All	All	All
Application	Oracle	Financial Services Data Integration Hub	8.0.6	All	All	All
Application	Oracle	Financial Services Data Integration Hub	8.0.3	All	All	All
Application	Oracle	Financial Services Data Integration Hub	8.0.6	All	All	All
Application	Oracle	Hospitality Opera 5	5.6	All	All	All
Application	Oracle	Mysql Enterprise Monitor	8.0.23	All	All	All

References

Reference

[CVE-2020-17530 Apache Struts Vulnerability in NetApp Products | NetApp Product Security](#)

[Oracle Critical Patch Update Advisory - April 2022](#)

[Oracle Critical Patch Update Advisory - July 2021](#)

[Oracle Critical Patch Update Advisory - October 2021](#)

[JVN#43969166: Apache Struts 2 vulnerable to remote code execution \(S2-061\)](#)

[Oracle Critical Patch Update Advisory - January 2022](#)

[S2-061 - Apache Struts 2 Wiki - Apache Software Foundation](#)

[oss-security - CVE-2021-31805: Apache Struts: Forced OGNL evaluation, when evaluated on raw not validated user input in tag attributes, ma](#)

[Apache Struts 2 Forced Multi OGNL Evaluation ≈ Packet Storm](#)

[Oracle Critical Patch Update Advisory - April 2021](#)

[Oracle Critical Patch Update Advisory - January 2021](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

[CISA Known Exploited Vulnerabilities catalog](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[150354 Apache Struts 2 Double OGNL Evaluation Vulnerability \(CVE-2020-17530\)](#)

© 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](#).

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