



CVE-2021-31805

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-31805
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-12 16:15:00 UTC
Updated	2022-07-25 18:15:00 UTC
Description	The fix issued for CVE-2020-17530 was incomplete. So from Apache Struts 2.0.0 to 2.5.29, still some of the tag's attributes

Risk And Classification

Problem Types: CWE-917

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Struts	All	All	All	All

References

Reference
S2-062 - Apache Struts 2 Wiki - Apache Software Foundation
CVE-2021-31805 Apache Struts Vulnerability in NetApp Products NetApp Product Security
oss-security - CVE-2021-31805: Apache Struts: Forced OGNL evaluation, when evaluated on raw not validated user input in tag attributes, ma
Oracle Critical Patch Update Advisory - July 2022
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Apache Struts would like to thank Chris McCown for reporting this issue!

Legacy QID Mappings

150504 Apache Struts 2 Remote Code Execution Vulnerability (CVE-2021-31805)

[376539](#) Apache Struts2 Remote Code Execution (RCE) Vulnerability (S2-062)

[376540](#) Apache Struts2 Remote Code Execution (RCE) Vulnerability (S2-062) (Tomcat Server Authentication Record)

© [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](#)