



# CVE-2019-0230

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

## Summary

<b>CVE</b>	CVE-2019-0230
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-09-14 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:01:00 UTC
<b>Description</b>	Apache Struts 2.0.0 to 2.5.20 forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead

## Risk And Classification

**Problem Types:** CWE-1321

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Struts</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Policy Management</a>	12.5.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Financial Services Data Integration Hub</a>	8.0.3	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Financial Services Data Integration Hub</a>	8.0.6	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Financial Services Data Integration Hub</a>	8.0.3	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Financial Services Data Integration Hub</a>	8.0.6	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Financial Services Market Risk Measurement And Management</a>	8.0.6	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Financial Services Market Risk Measurement And Management</a>	8.0.6	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Mysql Enterprise Monitor</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>	
S2-059 - Apache Struts 2 Wiki - Apache Software Foundation	MISC	<a href="#">cwiki.apache.org</a>	Vendor Advisory
Oracle Critical Patch Update Advisory - October 2021	MISC	<a href="#">www.oracle.com</a>	
launchpad.support.sap.com	MISC	<a href="#">launchpad.support.sap.com</a>	Permissions Required
Pony Mail!		<a href="#">lists.apache.org</a>	

Pony Mail!			<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!	MLIST		<a href="https://lists.apache.org">lists.apache.org</a>	Mailing List, Vendor Advisory
Apache Struts 2 Forced Multi OGNL Evaluation ≈ Packet Storm	MISC		<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	Exploit, Third Party Advisory, VI
Oracle Critical Patch Update Advisory - April 2021	MISC		<a href="https://www.oracle.com">www.oracle.com</a>	
Oracle Critical Patch Update Advisory - January 2021	MISC		<a href="https://www.oracle.com">www.oracle.com</a>	Third Party Advisory
Apache Struts 2.5.20 Double OGNL Evaluation ≈ Packet Storm	MISC		<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	Exploit, Third Party Advisory, VI
CVE Program record	CVE.ORG		<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD		<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[730436](#) Update TITLE manually (JRASERVER-71448)

[730443](#) Atlassian Jira Remote Code Execution (RCE) Vulnerability (JRASERVER-71448)

[730446](#) (JRASERVER-71448)

© [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](https://status.cve.report)