



# CVE-2021-37535

Published on: 09/14/2021 12:00:00 AM UTC

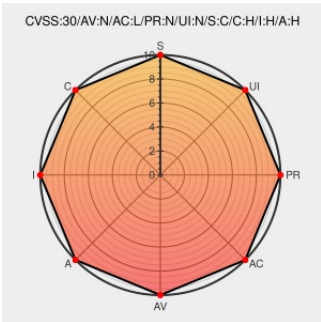
Last Modified on: 09/23/2021 08:00:00 PM UTC

## CVE-2021-37535

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Netweaver Application Server Java](#) from [Sap](#) contain the following vulnerability:

SAP NetWeaver Application Server Java (JMS Connector Service) - versions 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not perform necessary authorization checks for user privileges.

CVE-2021-37535 has been assigned by [sap](#) cna@sap.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>PARTIAL</b>	<b>PARTIAL</b>	<b>PARTIAL</b>

## CVE References

Description	Tags	Link
SAP Security Patch Day – September 2021 - Product Security Response at SAP - Community Wiki	<a href="#">wiki.scn.sap.com</a> <a href="#">text/html</a>	<a href="#">SAP</a> MISC <a href="#">wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=585106405</a>
<b>No Description Provided</b>	<a href="#">launchpad.support.sap.com</a>	<a href="#">SAP</a> MISC

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

## Related QID Numbers




87464 SAP NetWeaver AS Java JMS Missing Authorization Check Vulnerability

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	<a href="#">Netweaver Application Server Java</a>	7.11	All	All	All
Application	Sap	<a href="#">Netweaver Application Server Java</a>	7.20	All	All	All
Application	Sap	<a href="#">Netweaver Application Server Java</a>	7.30	All	All	All
Application	Sap	<a href="#">Netweaver Application Server Java</a>	7.31	All	All	All
Application	Sap	<a href="#">Netweaver Application Server Java</a>	7.40	All	All	All
Application	Sap	<a href="#">Netweaver Application Server Java</a>	7.50	All	All	All
cpe:2.3:a:sap:netweaver_application_server_java:7.11:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_application_server_java:7.20:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_application_server_java:7.30:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_application_server_java:7.31:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_application_server_java:7.40:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_application_server_java:7.50:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

## Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-37535 : #SAP NetWeaver Application Server Java JMS Connector Service - versions 7.11, 7.20, 7.30, 7.31,... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-09-14 12:09:54
 @ThreatMonIT	• [CVE-2021-37535] Missing Authorization check in SAP NetWeaver Application Server for Java (JMS Connector Service)... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-09-14 19:33:33
 @autumn_good_35	CVE-2021-37535とかヤバそうですね... SAP Security Patch Day – September 2021 <a href="https://wiki.scn.sap.com/wiki/pages/view...">wiki.scn.sap.com/wiki/pages/view...</a> <a href="https://t.co/PHfjJNJe1a">https://t.co/PHfjJNJe1a</a>	2021-09-15 06:02:23

[← Previous ID](#)

[Next ID →](#)

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](#)**