



CVE-2022-41212

Published on: Not Yet Published

Last Modified on: 11/09/2022 03:41:00 PM UTC

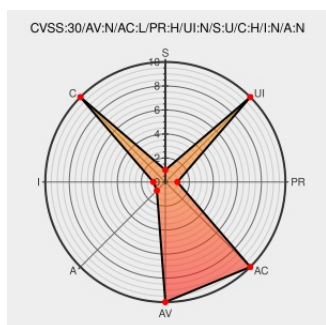
CVE-2022-41212

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to read a file which is otherwise restricted. On successful exploitation an attacker can completely compromise the confidentiality of the application.

CVE-2022-41212 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.9 - MEDIUM**

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

CVE References

Description	Tags	Link
Access Denied	www.sap.com text/html Inactive Link Not Archived	SAP MISC www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html
No Description Provided	launchpad.support.sap.com text/html	SAP MISC launchpad.support.sap.com/#/notes/3256571

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](#).

Related QID Numbers

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver Application Server Abap	700	All	All	All
Application	Sap	Netweaver Application Server Abap	731	All	All	All
Application	Sap	Netweaver Application Server Abap	740	All	All	All
Application	Sap	Netweaver Application Server Abap	750	All	All	All
Application	Sap	Netweaver Application Server Abap	789	All	All	All
Application	Sap	Netweaver Application Server Abap	804	All	All	All

cpe:2.3:a:sap:netweaver_application_server_abap:700:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:731:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:740:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:750:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:789:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:804:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2022-41212	2022-11-08 22:38:46

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)