



CVE-2023-24522

Published on: Not Yet Published

Last Modified on: 04/11/2023 10:15:00 PM UTC

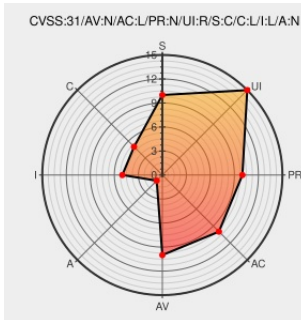
CVE-2023-24522

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 sanitization, SAP NetWeaver AS ABAP (Business Server Pages) - versions 700, 701, 702, 731, 740, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application.

CVE-2023-24522 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [SAP](#) **SAP - NetWeaver AS ABAP (BSP Framework)** version = 700

Affected Vendor/Software: [SAP](#) **SAP - NetWeaver AS ABAP (BSP Framework)** version = 701

Affected Vendor/Software: [SAP](#) **SAP - NetWeaver AS ABAP (BSP Framework)** version = 702

Affected Vendor/Software: [SAP](#) **SAP - NetWeaver AS ABAP (BSP Framework)** version = 731

Affected Vendor/Software: [SAP](#) **SAP - NetWeaver AS ABAP (BSP Framework)** version = 740

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
No Description Provided	launchpad.support.sap.com text/html	SAP MISC launchpad.support.sap.com/#/notes/3269118

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

87533 SAP NetWeaver AS ABAP and ABAP Cross-Site Scripting (XSS) Vulnerability

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	701	All	All	All
Application	Sap	Netweaver Application Server Abap	702	All	All	All
Application	Sap	Netweaver Application Server Abap	731	All	All	All
Application	Sap	Netweaver Application Server Abap	740	All	All	All
cpe:2.3:a:sap:netweaver_application_server_abap:700:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_application_server_abap:701:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_application_server_abap:702:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_application_server_abap:731:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_application_server_abap:740:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-24522 : Due to insufficient input sanitization, #SAP NetWeaver AS ABAP Business Server Pages - versions... twitter.com/i/web/status/1...	2023-02-14 04:10:30
 /r/netcve	CVE-2023-24522	2023-02-14 05:38:50

[← Previous ID](#)

[Next ID →](#)

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](#)