CVE-2022-29610

Published on: Not Yet Published

Last Modified on: 05/19/2022 03:18:00 AM UTC

CVE-2022-29610

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF

null

Certain versions of Netweaver Application Server Abap from Sap contain the following vulnerability:

SAP NetWeaver Application Server ABAP allows an authenticated attacker to upload malicious files and delete (theme) data, which could result in Stored Cross-Site Scripting (XSS) attack.

CVE-2022-29610 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver Application Server ABAP** version = **753**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver Application Server ABAP** version = **754**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver Application Server ABAP** version = **755**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver Application Server ABAP** version = **756**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Access Denied	www.sap.com text/html Inactive Link Not Archived	MISC www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html
No Description Provided	launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/3146336

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

87502 SAP NetWeaver AS 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	753	All	All	All
Application	Sap	Netweaver Application Server Abap	754	All	All	All
Application	Sap	Netweaver Application Server Abap	755	All	All	All
Application	Sap	Netweaver Application Server Abap	756	All	All	All

cpe:2.3:a:sap:netweaver_application_server_abap:753:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:754:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:755:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:756:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29610 : #SAP NetWeaver Application Server ABAP allows an authenticated attacker to upload malicious files… twitter.com/i/web/status/1…	2022-05-11 15:11:47
/r/netcve	CVE-2022-29610	2022-05-11 16:38:45

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report