



CVE-2021-40499

Published on: 10/12/2021 12:00:00 AM UTC

Last Modified on: 10/18/2021 06:37:00 PM UTC

CVE-2021-40499

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

null

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

Client-side printing services SAP Cloud Print Manager and SAPSprint for SAP NetWeaver Application Server for ABAP - versions 7.70, 7.70 PI, 7.70 BYD, allow an attacker to inject code that can be executed by the application. An attacker could thereby control the behavior of the application.

CVE-2021-40499 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver Application Server for ABAP (SAP Cloud Print Manager and SAPSprint)** version **7.70**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver Application Server for ABAP (SAP Cloud Print Manager and SAPSprint)** version **7.70 PI**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver Application Server for ABAP (SAP Cloud Print Manager and SAPSprint)** version **7.70BYD**

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description	Tags	Link
SAP Security Patch Day – October 2021 - Product Security Response at SAP - Community Wiki	wiki.scn.sap.com text/html	 MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=587169983
No Description Provided	launchpad.support.sap.com text/html	 MISC launchpad.support.sap.com/#/notes/3100882

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver Application Server Abap	7.70	All	All	All
Application	Sap	Netweaver Application Server Abap	7.70byd	All	All	All
Application	Sap	Netweaver Application Server Abap	7.70_pi	All	All	All
cpe:2.3:a:sap:netweaver_application_server_abap:7.70:*****:..						
cpe:2.3:a:sap:netweaver_application_server_abap:7.70byd:*****:..						
cpe:2.3:a:sap:netweaver_application_server_abap:7.70_pi:*****:..						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-40499 : Client-side printing services #SAP Cloud Print Manager and SAPSprint for SAP NetWeaver Application... twitter.com/i/web/status/1...	2021-10-12 14:44:46

[← Previous ID](#)[Next ID →](#)

