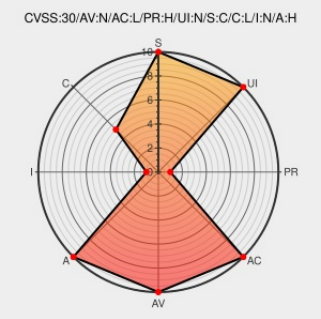
CVE-2020-26832

Published on: 12/09/2020 12:00:00 AM UTC

Last Modified on: 10/05/2022 02:21:00 PM UTC

CVE-2020-26832

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



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

SAP AS ABAP (SAP Landscape Transformation), versions - 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020 and SAP S4 HANA (SAP Landscape Transformation), versions - 101, 102, 103, 104, 105, allows a high privileged user to execute a RFC function module to which access should be restricted, however due to missing authorization an attacker can get access to some sensitive internal information of vulnerable SAP system or to make vulnerable SAP systems completely unavailable.

CVE-2020-26832 has been assigned by cna@sap.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.6 - HIGH

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link

SAP Security Patch Day – December 2020 - Product Security Response at SAP - Community Wiki	Vendor Advisory wiki.scn.sap.com text/html	MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564757079
No Description Provided	Permissions Required launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/2993132
SAP Application Server ABAP / ABAP Platform Code Injection / SQL Injection / Missing Authorization ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/167229/SAP-Application-Server-ABAP-ABAP-Platform-Code-Injection-SQL-Injection-Missing-Authorization.html
Full Disclosure: SEC Consult SA-20220518-0 :: Multiple Critical Vulnerabilities in SAP® Application Server, ABAP and ABAP® Platform (Different Software Components)	seclists.org text/html	FULLDISC 20220518 SEC Consult SA-20220518-0 :: Multiple Critical Vulnerabilities in SAP Application Server, ABAP and ABAP Platform (Different Software Components)

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	2011_1_620	All	All	All
Application	Sap	Netweaver Application Server Abap	2011_1_640	All	All	All
Application	Sap	Netweaver Application Server Abap	2011_1_700	All	All	All
Application	Sap	Netweaver Application Server Abap	2011_1_710	All	All	All
Application	Sap	Netweaver Application Server Abap	2011_1_730	All	All	All
Application	Sap	Netweaver Application Server Abap	2011_1_731	All	All	All
Application	Sap	Netweaver Application Server Abap	2011_1_752	All	All	All
Application	Sap	Netweaver Application Server Abap	2020	All	All	All
Application	Sap	Netweaver As Abap	2011_1_620	All	All	All
Application	Sap	Netweaver As Abap	2011_1_640	All	All	All
Application	Sap	Netweaver As Abap	2011_1_700	All	All	All
Application	Sap	Netweaver As Abap	2011_1_710	All	All	All
Application	Sap	Netweaver As Abap	2011_1_730	All	All	All
Application	Sap	Netweaver As Abap	2011_1_731	All	All	All
Application	Sap	Netweaver As Abap	2011_1_752	All	All	All
Application	Sap	Netweaver As Abap	2020	All	All	All
Application	Sap	Netweaver As Abap	2011_1_620	All	All	All

Application	Sap	Netweaver As Abap	2011_1_640	All	All	All
Application	Sap	Netweaver As Abap	2011_1_700	All	All	All
Application	Sap	Netweaver As Abap	2011_1_710	All	All	All
Application	Sap	Netweaver As Abap	2011_1_730	All	All	All
Application	Sap	Netweaver As Abap	2011_1_731	All	All	All
Application	Sap	Netweaver As Abap	2011_1_752	All	All	All
Application	Sap	Netweaver As Abap	2020	All	All	All
Application	Sap	S/4 Hana	101	All	All	All
Application	Sap	S/4 Hana	102	All	All	All
Application	Sap	S/4 Hana	103	All	All	All
Application	Sap	S/4 Hana	104	All	All	All
Application	Sap	S/4 Hana	105	All	All	All
Application	Sap	S/4 Hana	101	All	All	All
Application	Sap	S/4 Hana	102	All	All	All
Application	Sap	S/4 Hana	103	All	All	All
Application	Sap	S/4 Hana	104	All	All	All
Application	Sap	S/4 Hana	105	All	All	All

cpe:2.3:a:sap:netweaver_application_server_abap:2011_1_620:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:2011_1_640:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:2011_1_700:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:2011_1_710:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:2011_1_730:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:2011_1_731:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:2011_1_752:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:2020:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_620:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_640:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_700:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_710:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_730:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_731:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_752:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2020:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_620:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_640:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_700:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_710:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_730:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_731:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2011_1_752:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:2020:*:*:*:*:*:*:*:

cpe:2.3:a:sap:s\/4_hana:101:*:*:*:*:*:*:*:

cpe:2.3:a:sap:s\/4_hana:102:*:*:*:*:*:*:*:

cpe:2.3:a:sap:s\/4_hana:103:*:*:*:*:*:*:*:

cpe:2.3:a:sap:s\/4_hana:104:*:*:*:*:*:*:*:

cpe:2.3:a:sap:s\/4_hana:105:*:*:*:*:*:*:*:

cpe:2.3:a:sap:s\/4_hana:101:*:*:*:*:*:*:*:

cpe:2.3:a:sap:s\/4_hana:102:*:*:*:*:*:*:*:

cpe:2.3:a:sap:s\/4_hana:103:*:*:*:*:*:*:*:

cpe:2.3:a:sap:s\/4_hana:104:*:*:*:*:*:*:*:

cpe:2.3:a:sap:s\/4_hana:105:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ??? | SAP AS ABAP (SAP Landscape Transformatio... | CVE-2020-26832 | Link for more: alerts.remotelyrmm.com/CVE-2020-26832	2022-05-19 01:33:39

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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