

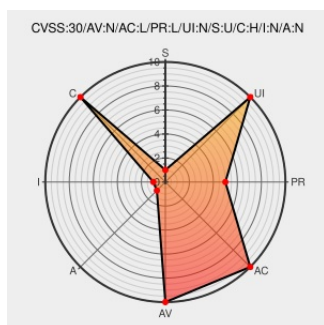


CVE-2020-26818

Published on: 11/10/2020 12:00:00 AM UTC

Last Modified on: 10/05/2022 02:16:00 PM UTC

CVE-2020-26818

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

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

SAP NetWeaver AS ABAP (Web Dynpro), versions - 731, 740, 750, 751, 752, 753, 754, 755, 782, allows an authenticated user to access Web Dynpro components, which reveals sensitive system information that would otherwise be restricted to highly privileged users because of missing authorization, resulting in Information Disclosure.

CVE-2020-26818 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SAP Security Patch Day – November 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=562725571

No Description Provided

Permissions Required

Vendor Advisory

launchpad.support.sap.com

text/html

 MISC

launchpad.support.sap.com/#/notes/2971954

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	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	751	All	All	All
Application	Sap	Netweaver Application Server Abap	752	All	All	All
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	782	All	All	All
Application	Sap	Netweaver As Abap	731	All	All	All
Application	Sap	Netweaver As Abap	740	All	All	All
Application	Sap	Netweaver As Abap	750	All	All	All
Application	Sap	Netweaver As Abap	751	All	All	All
Application	Sap	Netweaver As Abap	752	All	All	All
Application	Sap	Netweaver As Abap	753	All	All	All
Application	Sap	Netweaver As Abap	754	All	All	All
Application	Sap	Netweaver As Abap	755	All	All	All
Application	Sap	Netweaver As Abap	782	All	All	All
Application	Sap	Netweaver As Abap	731	All	All	All
Application	Sap	Netweaver As Abap	740	All	All	All
Application	Sap	Netweaver As Abap	750	All	All	All
Application	Sap	Netweaver As Abap	751	All	All	All
Application	Sap	Netweaver As Abap	752	All	All	All
Application	Sap	Netweaver As Abap	753	All	All	All
Application	Sap	Netweaver As Abap	754	All	All	All

Application	Sap	Netweaver As Abap	755	All	All	All
Application	Sap	Netweaver As Abap	782	All	All	All
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:751:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_application_server_abap:752:*:*:*:*:*.*:						
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:782:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:731:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:740:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:750:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:751:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:752:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:753:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:754:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:755:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:782:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:731:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:740:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:750:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:751:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:752:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:753:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:754:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver_as_abap:755:*:*:*:*:*.*:						
cpe:2.3:a:sap:netweaver as abap:782:*:*:*:*:*.*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @RemotelyAlerts	Severity: ?? SAP NetWeaver AS ABAP (Web Dynpro), vers... CVE-2020-26818 Link for more: alerts.remotelyrmm.com/CVE-2020-26818	2022-10-05 15:29:16

[← 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