

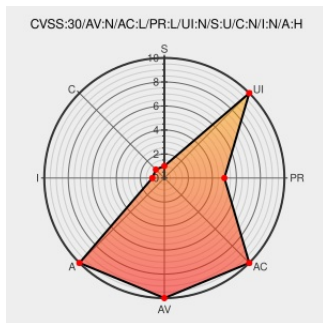


CVE-2020-26826

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

Last Modified on: 03/23/2021 11:23:56 PM UTC

CVE-2020-26826

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

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

Process Integration Monitoring of SAP NetWeaver AS JAVA, versions - 7.31, 7.40, 7.50, allows an attacker to upload any file (including script files) without proper file format validation, leading to Unrestricted File Upload.

CVE-2020-26826 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver AS JAVA** version 7.31

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver AS JAVA** version 7.40

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver AS JAVA** version 7.50

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

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	SAP MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pagelId=564757079
No Description Provided	Permissions Required launchpad.support.sap.com text/html	SAP MISC launchpad.support.sap.com/#/notes/2974330

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

87517 SAP NetWeaver AS for Java Arbitrary File Upload Vulnerability.

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver Application Server Java	7.31	All	All	All
Application	Sap	Netweaver Application Server Java	7.40	All	All	All
Application	Sap	Netweaver Application Server Java	7.50	All	All	All
Application	Sap	Netweaver Application Server Java	7.31	All	All	All
Application	Sap	Netweaver Application Server Java	7.40	All	All	All
Application	Sap	Netweaver Application Server Java	7.50	All	All	All
cpe:2.3:a:sap:netweaver_application_server_java:7.31:*****:						
cpe:2.3:a:sap:netweaver_application_server_java:7.40:*****:						
cpe:2.3:a:sap:netweaver_application_server_java:7.50:*****:						
cpe:2.3:a:sap:netweaver_application_server_java:7.31:*****:						
cpe:2.3:a:sap:netweaver_application_server_java:7.40:*****:						
cpe:2.3:a:sap:netweaver_application_server_java:7.50:*****:						

No vendor comments have been submitted for this CVE

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](#)