



CVE-2020-26820

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

Last Modified on: 01/01/2022 06:18:00 PM UTC

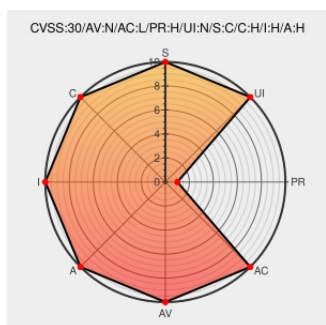
CVE-2020-26820

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

SAP NetWeaver AS JAVA, versions - 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker who is authenticated as an administrator to use the administrator console, to expose unauthenticated access to the file system and upload a malicious file. The attacker or another user can then use a separate mechanism to execute OS commands through the uploaded file leading to Privilege Escalation and completely compromise the confidentiality, integrity and availability of the server operating system and any application running on it.

CVE-2020-26820 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver AS JAVA** version 7.20

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver AS JAVA** version 7.30

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: **7.2 - HIGH**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication

Network	Low	Single
Confidentiality Impact	Integrity Impact	Availability Impact
Complete	Complete	Complete

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?pagelId=562725571
SAP Java OS Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/162086/SAP-Java-OS-Remote-Code-Execution.html
Full Disclosure: Onapsis Security Advisory 2021-0004: [CVE-2020-26820] - SAP Java OS Remote Code Execution	seclists.org text/html	 FULLDISC 20210405 Onapsis Security Advisory 2021-0004: [CVE-2020-26820] - SAP Java OS Remote Code Execution
No Description Provided	Permissions Required Vendor Advisory launchpad.support.sap.com text/html	 MISC launchpad.support.sap.com/#!/notes/2979062

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

87459 SAP NetWeaver AS Java Remote Code Execution Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver Application Server Java	7.20	All	All	All
Application	Sap	Netweaver Application Server Java	7.30	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
Application	Sap	Netweaver Application Server Java	7.20	All	All	All
Application	Sap	Netweaver Application Server Java	7.30	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:7.20:*:*:*:*:*:						
cpe:2.3:a:sap:netweaver_application_server_java:7.30:*:*:*:*:*:						

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:7.20:*****:
cpe:2.3:a:sap:netweaver_application_server_java:7.30:*****:
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

Social Mentions		
Source	Title	Posted (UTC)
 /r/bag_o_news	Onapsis Security Advisory 2021-0004: [CVE-2020-26820] - SAP Java OS Remote Code Execution	2021-04-06 15:21:13
← Previous ID Next ID→		