



CVE-2020-6224

Published on: 04/14/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

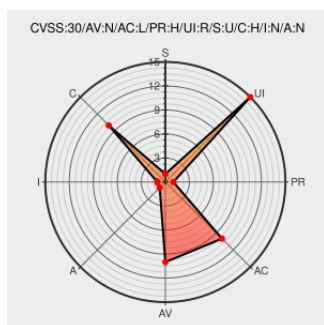
CVE-2020-6224

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 (HTTP Service), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker with administrator privileges to access user sensitive data such as passwords in trace files, when the user logs in and sends request with login credentials, leading to Information Disclosure.

CVE-2020-6224 has been assigned by [sap](#) cna@sap.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.2 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link
No Description Provided	Permissions Required Vendor Advisory launchpad.support.sap.com	SAP MISC launchpad.support.sap.com/#/notes/2826528

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

87516 SAP NetWeaver AS for Java Information Disclosure Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver Application Server Java	7.10	All	All	All
Application	Sap	Netweaver Application Server Java	7.11	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
Application	Sap	Netweaver Application Server Java	7.10	All	All	All
Application	Sap	Netweaver Application Server Java	7.11	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:7.10:*****:

cpe:2.3:a:sap:netweaver_application_server_java:7.11:*****:

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:7.10:*****:

cpe:2.3:a:sap:netweaver_application_server_java:7.11:*****:	
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	
← Previous ID	Next ID →