

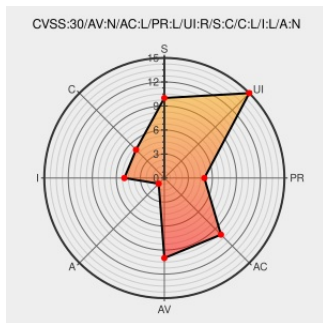


CVE-2020-6313

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

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

CVE-2020-6313

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

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

SAP NetWeaver Application Server JAVA(XML Forms) versions 7.30, 7.31, 7.40, 7.50 does not sufficiently encode user controlled inputs, which allows an authenticated User with special roles to store malicious content, that when accessed by a victim, can perform malicious actions by executing JavaScript, leading to Stored Cross-Site Scripting.

CVE-2020-6313 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 (XML Forms)** version **7.30**

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

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

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver AS JAVA (XML Forms)** 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	HIGH	NONE

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
SAP Security Patch Day – September 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=557449700
No Description Provided	Permissions Required launchpad.support.sap.com text/html	 MISC launchpad.support.sap.com/#/notes/2953112

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

[87515](#) SAP NetWeaver AS for Java Stored Cross-Site Scripting (XSS) Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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 Knowledge Management	7.30	All	All	All
Application	Sap	Netweaver Knowledge Management	7.31	All	All	All
Application	Sap	Netweaver Knowledge Management	7.40	All	All	All
Application	Sap	Netweaver Knowledge Management	7.50	All	All	All
Application	Sap	Netweaver Knowledge Management	7.30	All	All	All
Application	Sap	Netweaver Knowledge Management	7.31	All	All	All
Application	Sap	Netweaver Knowledge Management	7.40	All	All	All
Application	Sap	Netweaver Knowledge Management	7.50	All	All	All

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_knowledge_management:7.30:*****:

cpe:2.3:a:sap:netweaver_knowledge_management:7.31:*****:

cpe:2.3:a:sap:netweaver_knowledge_management:7.40:*****:
cpe:2.3:a:sap:netweaver_knowledge_management:7.50:*****:
cpe:2.3:a:sap:netweaver_knowledge_management:7.30:*****:
cpe:2.3:a:sap:netweaver_knowledge_management:7.31:*****:
cpe:2.3:a:sap:netweaver_knowledge_management:7.40:*****:
cpe:2.3:a:sap:netweaver_knowledge_management:7.50:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)