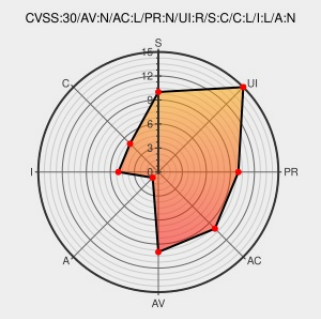
CVE-2020-6319

Published on: 10/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:04 PM UTC

CVE-2020-6319

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, versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, and 7.50 allows an unauthenticated attacker to include JavaScript blocks in any web page or URL with different symbols which are otherwise not allowed. On successful exploitation an attacker can steal authentication information of the user, such as data relating to his or her current session and limitedly impact confidentiality and integrity of the application, leading to Reflected Cross Site Scripting.

CVE-2020-6319 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
SAP Security Patch Day – October 2020 – Product Security	Vendor Advisory	MISC

SAP Security Patch Day – October 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=558632196
No Description Provided	Permissions Required launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/2956398

Related QID Numbers

87514 SAP NetWeaver AS for Java Reflected Cross-Site Scripting (XSS) Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver Application Server Java	7.10	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→