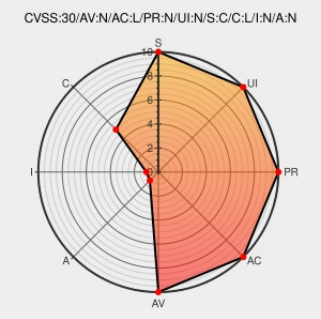
CVE-2020-6282

Published on: 07/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:05 PM UTC

CVE-2020-6282

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 (IIOP service) (SERVERCORE), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, and SAP NetWeaver AS JAVA (IIOP service) (CORE-TOOLS), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker to send a crafted request from a vulnerable web application. It is usually used to target internal systems behind firewalls that are normally inaccessible to an attacker from the external network, resulting in a Server-Side Request Forgery vulnerability.

CVE-2020-6282 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.8 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided.	Permissions Required	MISC

No Description Provided	Permissions Required Vendor Advisory launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/2896025
SAP Security Patch Day – July 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=552599675

Related QID Numbers

87495 SAP NetWeaver AS Server-Side Request Forgery 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→