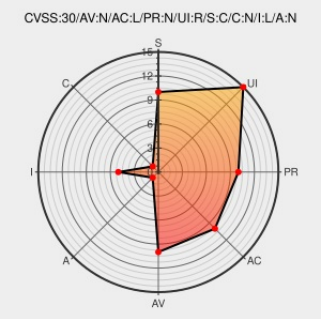
CVE-2020-6365

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

Last Modified on: 04/12/2021 02:21:00 PM UTC

CVE-2020-6365

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Netweaver from Sap contain the following vulnerability:

SAP NetWeaver AS Java, versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, Start Page allows an unauthenticated remote attacker to redirect users to a malicious site due to insufficient reverse tabnabbing URL validation. The attacker could execute phishing attacks to steal credentials of the victim or to redirect users to untrusted web pages containing malware or similar malicious exploits.

CVE-2020-6365 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: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
SAP Security Patch Day – October 2020 - Product Security Response at SAP - Community Wiki	Vendor Advisory wiki.scn.sap.com	MISC wiki.scn.sap.com/wiki/pages/viewpage.action?

	text/html	pageId=558632196
No Description Provided	Permissions Required Vendor Advisory launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/2969828

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver	application_server_java	7.10	All	All
Application	Sap	Netweaver	application_server_java	7.20	All	All
Application	Sap	Netweaver	application_server_java	7.30	All	All
Application	Sap	Netweaver	application_server_java	7.31	All	All
Application	Sap	Netweaver	application_server_java	7.40	All	All
Application	Sap	Netweaver	application_server_java	7.50	All	All
Application	Sap	Netweaver	application_server_java	7.10	All	All
Application	Sap	Netweaver	application_server_java	7.20	All	All
Application	Sap	Netweaver	application_server_java	7.30	All	All
Application	Sap	Netweaver	application_server_java	7.31	All	All
Application	Sap	Netweaver	application_server_java	7.40	All	All
Application	Sap	Netweaver	application_server_java	7.50	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:7.20:*:*:*:*:*:*:*

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:7.20:*:*:*:*:*:*:*

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

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→