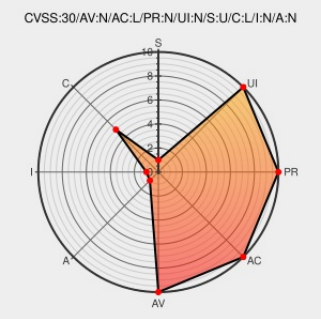
CVE-2020-6286

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

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

CVE-2020-6286

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



Certain versions of Netweaver Application Server Java from Sap contain the following vulnerability:

The insufficient input path validation of certain parameter in the web service of SAP NetWeaver AS JAVA (LM Configuration Wizard), versions - 7.30, 7.31, 7.40, 7.50, allows an unauthenticated attacker to exploit a method to download zip files to a specific directory, leading to Path Traversal.

CVE-2020-6286 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver AS JAVA (LM Configuration Wizard)** version **7.30**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver AS JAVA (LM Configuration Wizard)** version **7.31**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver AS JAVA (LM Configuration Wizard)** version **7.40**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver AS JAVA (LM Configuration Wizard)** version **7.50**

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	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 Vendor Advisory launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/2934135
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

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoC for CVE-2020-6287, CVE-2020-6286 (SAP RECON 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 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:7.30:*:*:*:*:*:*:*

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:7.30:*:*:*:*:*:*:*

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→