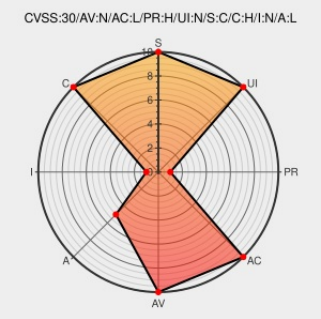
CVE-2020-6366

Published on: 10/20/2020 12:00:00 AM UTC

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

CVE-2020-6366

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



Certain versions of Netweaver Compare Systems from Sap contain the following vulnerability:

SAP NetWeaver (Compare Systems) versions - 7.20, 7.30, 7.40, 7.50, does not sufficiently validate uploaded XML documents. An attacker with administrative privileges can retrieve arbitrary files including files on OS level from the server and/or can execute a denial-of-service.

CVE-2020-6366 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver (Compare Systems)** version **7.20**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver (Compare Systems)** version **7.30**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver (Compare Systems)** version **7.31**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver (Compare Systems)** version **7.40**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver (Compare Systems)** version **7.50**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 5.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL | NONE | PARTIAL

CVE References

Description	Tags	Link
No Description Provided	Permissions Required Vendor Advisory launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/2969457
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

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 Compare Systems	7.20	All	All	All
Application	Sap	Netweaver Compare Systems	7.30	All	All	All
Application	Sap	Netweaver Compare Systems	7.31	All	All	All
Application	Sap	Netweaver Compare Systems	7.40	All	All	All
Application	Sap	Netweaver Compare Systems	7.50	All	All	All
Application	Sap	Netweaver Compare Systems	7.20	All	All	All
Application	Sap	Netweaver Compare Systems	7.30	All	All	All
Application	Sap	Netweaver Compare Systems	7.31	All	All	All
Application	Sap	Netweaver Compare Systems	7.40	All	All	All
Application	Sap	Netweaver Compare Systems	7.50	All	All	All

cpe:2.3:a:sap:netweaver_compare_systems:7.20:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_compare_systems:7.30:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_compare_systems:7.31:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_compare_systems:7.40:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_compare_systems:7.50:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_compare_systems:7.20:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_compare_systems:7.30:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_compare_systems:7.31:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_compare_systems:7.40:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_compare_systems:7.50:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→