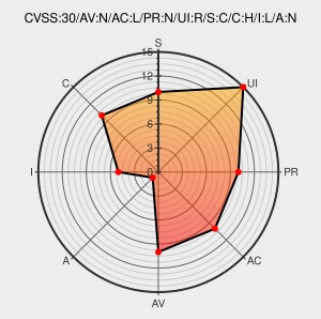
CVE-2020-6367

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

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

CVE-2020-6367

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



Certain versions of Netweaver Composite Application Framework from Sap contain the following vulnerability:

There is a reflected cross site scripting vulnerability in SAP NetWeaver Composite Application Framework, versions - 7.20, 7.30, 7.31, 7.40, 7.50. An unauthenticated attacker can trick an unsuspecting authenticated user to click on a malicious link. The end users browser has no way to know that the script should not be trusted, and will execute the script, resulting in sensitive information being disclosed or modified.

CVE-2020-6367 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver Composite Application Framework** version **7.20**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver Composite Application Framework** version **7.30**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver Composite Application Framework** version **7.31**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver Composite Application Framework** version **7.40**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver Composite Application Framework** version **7.50**

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 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 Vendor Advisory launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/2972661

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 Composite Application Framework	7.20	All	All	All
Application	Sap	Netweaver Composite Application Framework	7.30	All	All	All
Application	Sap	Netweaver Composite Application Framework	7.31	All	All	All
Application	Sap	Netweaver Composite Application Framework	7.40	All	All	All
Application	Sap	Netweaver Composite Application Framework	7.50	All	All	All
Application	Sap	Netweaver Composite Application Framework	7.20	All	All	All
Application	Sap	Netweaver Composite Application Framework	7.30	All	All	All
Application	Sap	Netweaver Composite Application Framework	7.31	All	All	All
Application	Sap	Netweaver Composite Application Framework	7.40	All	All	All
Application	Sap	Netweaver Composite Application Framework	7.50	All	All	All

cpe:2.3:a:sap:netweaver_composite_application_framework:7.20:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_composite_application_framework:7.30:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_composite_application_framework:7.31:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_composite_application_framework:7.40:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_composite_application_framework:7.50:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_composite_application_framework:7.20:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_composite_application_framework:7.30:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_composite_application_framework:7.31:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_composite_application_framework:7.40:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_composite_application_framework:7.50:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→