



CVE-2020-6370

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

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

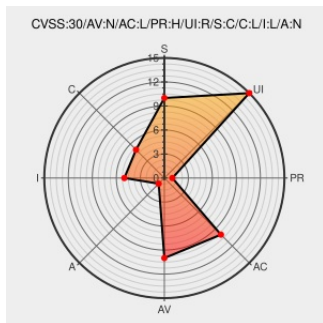
CVE-2020-6370

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Netweaver Design Time Repository](#) from [Sap](#) contain the following vulnerability:

SAP NetWeaver Design Time Repository (DTR), versions - 7.11, 7.30, 7.31, 7.40, 7.50, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.

CVE-2020-6370 has been assigned by [sap](#) cna@sap.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver (DI Design Time Repository)** version **7.11**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver (DI Design Time Repository)** version **7.30**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver (DI Design Time Repository)** version **7.31**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver (DI Design Time Repository)** version **7.40**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver (DI Design Time Repository)** version **7.50**

CVSS3 Score: **4.8 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description	Tags	Link
No Description Provided	Permissions Required Vendor Advisory launchpad.support.sap.com text/html	 MISC launchpad.support.sap.com/#/notes/2939419
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?pagelD=558632196

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 Design Time Repository	7.11	All	All	All
Application	Sap	Netweaver Design Time Repository	7.30	All	All	All
Application	Sap	Netweaver Design Time Repository	7.31	All	All	All
Application	Sap	Netweaver Design Time Repository	7.40	All	All	All
Application	Sap	Netweaver Design Time Repository	7.50	All	All	All
Application	Sap	Netweaver Design Time Repository	7.11	All	All	All
Application	Sap	Netweaver Design Time Repository	7.30	All	All	All
Application	Sap	Netweaver Design Time Repository	7.31	All	All	All
Application	Sap	Netweaver Design Time Repository	7.40	All	All	All
Application	Sap	Netweaver Design Time Repository	7.50	All	All	All
cpe:2.3:a:sap:netweaver_design_time_repository:7.11:****.*.*.*:						
cpe:2.3:a:sap:netweaver_design_time_repository:7.30:****.*.*.*:						
cpe:2.3:a:sap:netweaver_design_time_repository:7.31:****.*.*.*:						
cpe:2.3:a:sap:netweaver_design_time_repository:7.40:****.*.*.*:						
cpe:2.3:a:sap:netweaver_design_time_repository:7.50:****.*.*.*:						
cpe:2.3:a:sap:netweaver_design_time_repository:7.11:****.*.*.*:						
cpe:2.3:a:sap:netweaver_design_time_repository:7.30:****.*.*.*:						
cpe:2.3:a:sap:netweaver design time repository:7.31:****.*.*.*:						

</