

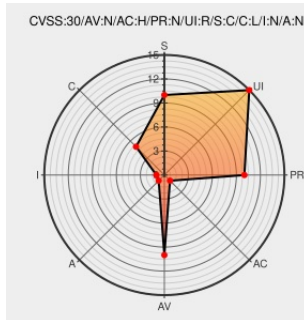


CVE-2020-26836

Published on: 12/09/2020 12:00:00 AM UTC

Last Modified on: 06/17/2021 05:18:00 PM UTC

CVE-2020-26836

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Solution Manager](#) from [Sap](#) contain the following vulnerability:

SAP Solution Manager (Trace Analysis), version - 720, allows for misuse of a parameter in the application URL leading to Open Redirect vulnerability, an attacker can enter a link to malicious site which could trick the user to enter credentials or download malicious software, as a parameter in the application URL and share it with the end user who could potentially become a victim of the attack.

CVE-2020-26836 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Solution Manager (Trace Analysis)** version 720

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 Solution Manager 7.2 (ST 720) Open Redirection ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/163136/SAP-Solution-Manager-7.2-ST-720-Open-Redirection.html
SAP Security Patch Day – December 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=564757079
Full Disclosure: Onapsis Security Advisory 2021-0005: SAP Solution Manager Open Redirect from Trace Analysis	seclists.org text/html	 FULLDISC 20210614 Onapsis Security Advisory 2021-0005: SAP Solution Manager Open Redirect from Trace Analysis
No Description Provided	Permissions Required launchpad.support.sap.com text/html	 MISC launchpad.support.sap.com/#/notes/2938650

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	Solution Manager	7.20	All	All	All
Application	Sap	Solution Manager	7.20	All	All	All
cpe:2.3:a:sap:solution_manager:7.20:*:*:*:*:*:						
cpe:2.3:a:sap:solution_manager:7.20:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous ID Next ID→		