



CVE-2020-26837

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

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

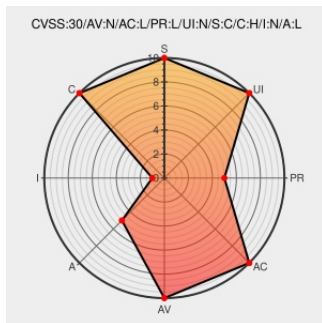
CVE-2020-26837

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

SAP Solution Manager 7.2 (User Experience Monitoring), version - 7.2, allows an authenticated user to upload a malicious script that can exploit an existing path traversal vulnerability to compromise confidentiality exposing elements of the file system, partially compromise integrity allowing the modification of some configurations and partially compromise availability by making certain services unavailable.

CVE-2020-26837 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Solution Manager (User Experience Monitoring)** version 7.20

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

No Description Provided	Permissions Required launchpad.support.sap.com text/html	 MISC launchpad.support.sap.com/#!/notes/2983204
SAP Solution Manager 7.2 File Disclosure / Denial Of Service ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/163160/SAP-Solution-Manager-7.2-File-Disclosure-Denial-Of-Service.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?pagelId=564757079
Full Disclosure: Onapsis Security Advisory 2021-0010: File exfiltration and DoS in SolMan End-User Experience Monitoring	seclists.org text/html	 FULLDISC 20210614 Onapsis Security Advisory 2021-0010: File exfiltration and DoS in SolMan End-User Experience Monitoring
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→		