

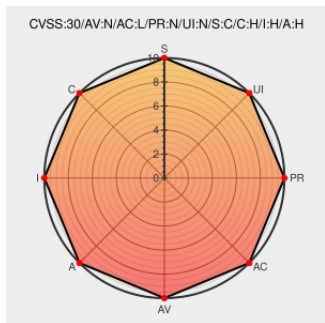


CVE-2020-6207

Published on: 03/10/2020 12:00:00 AM UTC

Last Modified on: 06/17/2021 02:30:00 PM UTC

CVE-2020-6207

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

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

SAP Solution Manager (User Experience Monitoring), version- 7.2, due to Missing Authentication Check does not perform any authentication for a service resulting in complete compromise of all SMDAgents connected to the Solution Manager.

CVE-2020-6207 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 7.2

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
SAP Solution Manager 7.2 Remote Command Execution ~ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/161993/SAP-Solution-Manager-7.2-Remote-Command-

SAP SMD Agent Unauthenticated Remote Code Execution ≈ Packet Storm

[packetstormsecurity.com](https://packetstormsecurity.com/text/html)
text/html

 MISC
packetstormsecurity.com/files/162083/SAP-SMD-Agent-Unauthenticated-Remote-Code-Execution.html

Full Disclosure: Onapsis Security Advisory 2021-0001: [CVE-2020-6207] - Unauthenticated RCE in SAP all SMD Agents connected to SAP SolMan

[seclists.org](https://seclists.org/text/html)
text/html

 FULLDISC 20210405 Onapsis Security Advisory 2021-0001: [CVE-2020-6207] - Unauthenticated RCE in SAP all SMD Agents connected to SAP SolMan

SAP Solution Manager 7.20 Missing Authorization ≈ Packet Storm

[packetstormsecurity.com](https://packetstormsecurity.com/text/html)
text/html

 MISC
packetstormsecurity.com/files/163168/SAP-Solution-Manager-7.20-Missing-Authorization.html

No Description Provided

Permissions Required
[launchpad.support.sap.com](https://launchpad.support.sap.com/text/html)
text/html

 MISC
launchpad.support.sap.com/#/notes/2890213

Full Disclosure: Onapsis Security Advisory 2021-0014: Missing authorization check in SAP Solution Manager LM-SERVICE Component SP 11 PL 2

[seclists.org](https://seclists.org/text/html)
text/html

 FULLDISC 20210614 Onapsis Security Advisory 2021-0014: Missing authorization check in SAP Solution Manager LM-SERVICE Component SP 11 PL 2

SAP Security Patch Day – March 2020 - Product Security Response at SAP - Community Wiki

Vendor Advisory
[wiki.scn.sap.com](https://wiki.scn.sap.com/text/html)
text/html

 MISC
wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=540935305

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

Exploit/POC from Github

PoC for CVE-2020-6207 (Missing Authentication Check in SAP Solution Manager)

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)
--------	-------	--------------

 @CyberSquarePeg	cnbcm.com/2021/04/05/goo... Whelp...make sure you are up to date on the software/patching! CVE-2020-6207, CVE-2018-2... twitter.com/i/web/status/1...	2021-04-06 15:47:11
 @tempest_sec	As falhas são: CVE-2020-6287 (CVSS 10), CVE-2020-6207 (CVSS 9.8), CVE-2018-2380 (CVSS 6.6), CVE-2016-3976 (CVSS 7.5... twitter.com/i/web/status/1...	2021-04-07 17:12:18
 @rimpq	?Couple of new #SIGMA rules to cover exploitation of CVE-2020-6287 / #CVE-2020-6207 SAP #vulnerabilities. (processe... twitter.com/i/web/status/1...	2021-04-08 12:33:02
 @Grego_Jf	CVE-2020-6287: apps.support.sap.com/sap/support/kn... CVE-2020-6207: CVE-2018-2380: ... twitter.com/i/web/status/1...	2021-04-09 03:24:36
 @blueteamsec1	[PDF] ONAPSIS: Active Cyberattacks on Mission-Critical SAP Applications - CVE-2020-6287, CVE-2020-6207, CVE-2018-23... twitter.com/i/web/status/1...	2021-04-16 12:09:02
 @rythensec	CVE-2020-6207 exploitation detected ?? 222.190.251.170 https://t.co/mODiW8co84	2022-03-27 02:56:19
 /r/bag_o_news	Onapsis Security Advisory 2021-0001: [CVE-2020-6207] - Unauthenticated RCE in SAP all SMD Agents connected to SAP SolMan	2021-04-06 15:21:27
 /r/blueteamsec	[PDF] ONAPSIS: Active Cyberattacks on Mission-Critical SAP Applications - CVE-2020-6287, CVE-2020-6207, CVE-2018-2380, CVE-2016-9563, CVE-2016-3976 and CVE-2010-5326	2021-04-07 11:10:22

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)