



CVE-2022-29527

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:22:00 PM UTC

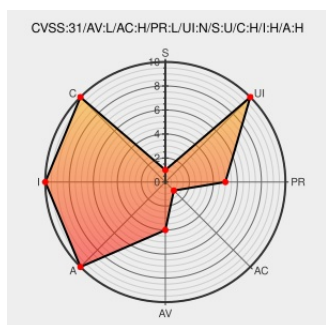
CVE-2022-29527

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Amazon Ssm Agent](#) from [Amazon](#) contain the following vulnerability:

Amazon AWS amazon-ssm-agent before 3.1.1208.0 creates a world-writable sudoers file, which allows local attackers to inject Sudo rules and escalate privileges to root. This occurs in certain situations involving a race condition.

CVE-2022-29527 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7 - HIGH**

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

CVSS2 Score: **6.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Bug 1196556 – VUL-0: amazon-ssm-agent: creates world-writable sudoers file during runtime (race condition)	bugzilla.suse.com text/html	MISC bugzilla.suse.com/show_bug.cgi?id=1196556
Release Amazon SSM Agent - Release 3.1.1208.0 -	github.com	MISC github.com/aws/amazon-ssm-

2022-04-04 · aws/amazon-ssm-agent · GitHub

text/html

agent/releases/tag/3.1.1208.0

Create ssm-agent-users sudoer file with constrained file permission · aws/amazon-ssm-agent@0fe8ae9 · GitHub

github.com

text/html

MISC github.com/aws/amazon-ssm-agent/commit/0fe8ae99b2ff25649c7b86d3bc05fc037400aca7

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.

Related QID Numbers

753381 SUSE Enterprise Linux Security Update for amazon-ssm-agent (SUSE-SU-2022:1510-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Amazon	Amazon Ssm Agent	All	All	All	All

cpe:2.3:a:amazon:amazon_ssm_agent:*.***:*.***:.*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29527 : Amazon AWS amazon-ssm-agent before 3.1.1208.0 creates a world-writable sudoers file, which allows... twitter.com/i/web/status/1...	2022-04-20 10:03:45
/r/netcve	CVE-2022-29527	2022-04-20 11:38:52
/r/InfoSecNews	Top 10 Most Interesting CVEs for April 2022	2022-05-05 09:59:31

← Previous ID

Next ID→