



CVE-2022-2385

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-2385
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-12 19:15:00 UTC
Updated	2022-07-19 17:20:00 UTC
Description	A security issue was discovered in aws-iam-authenticator where an allow-listed IAM identity may be able to modify their use

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubernetes	Aws-iam-authenticator	All	All	All	All

References

Reference	Source	Link
[Security Advisory] CVE-2022-2385: AccessKeyID validation bypass	MISC	groups.google
CVE-2022-2385: AccessKeyID validation bypass · Issue #472 · kubernetes-sigs/aws-iam-authenticator · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Gafnit Amiga

Legacy QID Mappings

[753317](#) SUSE Enterprise Linux Security Update for aws-iam-authenticator (SUSE-SU-2022:2583-1)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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