



Improper S3 ownership verification in Bedrock AgentCore Starter Toolkit

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

Summary

CVE	CVE-2026-4269
State	PUBLISHED
Assigner	AMZN
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-16 18:16:11 UTC
Updated	2026-05-11 14:34:12 UTC
Description	A missing S3 ownership verification in the Bedrock AgentCore Starter Toolkit before version v0.1.13 may allow a remote ac

Risk And Classification

Primary CVSS: v4.0 5.8 MEDIUM from ff89ba41-3aa1-4d27-914a-91399e9639e5

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000590000 probability, percentile 0.183640000 (date 2026-05-12)

Problem Types: CWE-283 | CWE-340 | CWE-340 CWE-340 Generation of Predictable Numbers or Identifiers | CWE-283 CWE-283 Unverified Ownership

Version	Source	Type	Score	Severity	Vector
4.0	ff89ba41-3aa1-4d27-914a-91399e9639e5	Secondary	5.8	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:N/VA
4.0	CNA	CVSS	5.8	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:N/VA
3.1	ff89ba41-3aa1-4d27-914a-91399e9639e5	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Amazon	Bedrock Agentcore Starter Toolkit	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	AWS	Bedrock AgentCore Starter Toolkit	affected 0.1.0 0.1.13 custom	Not specified

References

Reference	Source	Link	Tags
aws.amazon.com/security/security-bulletins/2026-008-AWS	ff89ba41-3aa1-4d27-914a-91399e9639e5	aws.amazon.com	Venc
github.com/aws/bedrock-agentcore-starter-toolkit/releases/tag/v0.1.13	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com	Rele
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report