Key commitment policy bypass via shared key cache in AWS Encryption SDK for Python

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-6550
State	PUBLISHED
Assigner	AMZN
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-20 20:16:49 UTC
Updated	2026-04-20 20:16:49 UTC
Description	Cryptographic algorithm downgrade in the caching layer of Amazon AWS Encryption SDK for Python before version 3.3.1 a

Risk And Classification

Primary CVSS: v4.0 5.7 MEDIUM from ff89ba41-3aa1-4d27-914a-91399e9639e5

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

Problem Types: CWE-757 | CWE-757 CWE-757 Selection of Less-Secure algorithm during negotiation ('algorithm downgrade')

Version	Source	Type	Score	Severity	Vector
4.0	ff89ba41-3aa1-4d27-914a-91399e9639e5	Secondary	5.7	MEDIUM	CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:N/VI:H/VA:
4.0	CNA	CVSS	5.7	MEDIUM	CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:N/VI:H/VA:
3.1	ff89ba41-3aa1-4d27-914a-91399e9639e5	Secondary	4.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	CVSS	4.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	AWS	AWS Encryption SDK For Python	affected 2 2.5.1 custom	Not specified
CNA	AWS	AWS Encryption SDK For Python	affected 3 3.3.0 custom	Not specified
CNA	AWS	AWS Encryption SDK For Python	affected 4 4.0.4 custom	Not specified

References

Reference	Source	Link
github.com/aws/aws-encryption-sdk-python/releases/tag/v3.3.1	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com
github.com/aws/aws-encryption-sdk-python/releases/tag/v4.0.5	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com
github.com/aws/aws-encryption-sdk-python/security/advisories/GHSA-v638-3...	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com
aws.amazon.com/security/security-bulletins/2026-017-aws	ff89ba41-3aa1-4d27-914a-91399e9639e5	aws.amazon.cc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: 1seal.org (en)

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