



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

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

## Summary

<b>CVE</b>	CVE-2026-6550
<b>State</b>	PUBLISHED
<b>Assigner</b>	AMZN
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-20 20:16:49 UTC
<b>Updated</b>	2026-04-20 20:16:49 UTC
<b>Description</b>	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/MSX/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: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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
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: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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
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/MSX: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
<a href="https://github.com/aws/aws-encryption-sdk-python/releases/tag/v3.3.1">github.com/aws/aws-encryption-sdk-python/releases/tag/v3.3.1</a>	ff89ba41-3aa1-4d27-914a-91399e9639e5	<a href="https://github.com">github.com</a>
<a href="https://github.com/aws/aws-encryption-sdk-python/releases/tag/v4.0.5">github.com/aws/aws-encryption-sdk-python/releases/tag/v4.0.5</a>	ff89ba41-3aa1-4d27-914a-91399e9639e5	<a href="https://github.com">github.com</a>
<a href="https://github.com/aws/aws-encryption-sdk-python/security/advisories/GHSA-v638-3...">github.com/aws/aws-encryption-sdk-python/security/advisories/GHSA-v638-3...</a>	ff89ba41-3aa1-4d27-914a-91399e9639e5	<a href="https://github.com">github.com</a>
<a href="https://aws.amazon.com/security/security-bulletins/2026-017-aws">aws.amazon.com/security/security-bulletins/2026-017-aws</a>	ff89ba41-3aa1-4d27-914a-91399e9639e5	<a href="https://aws.amazon.com">aws.amazon.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

## Vendor Comments And Credit

### Discovery Credit

**CNA:** 1seal.org (en)

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

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)