CVE-2026-6550 - Key commitment policy bypass via shared key cache in AWS Encryption SDK for Python

Bulletin ID: 2026-017-AWS
Scope: AWS
Content Type: Important (requires attention)
Publication Date: 04/20/2026 9:15 AM PDT

Description:

AWS Encryption SDK (ESDK) for Python is a client-side encryption library. We identified CVE-2026-6550, which describes an issue with a key commitment policy bypass via shared key cache.

Cryptographic algorithm downgrade in the caching layer of Amazon AWS Encryption SDK for Python before version 3.3.1 and before version 4.0.5 might allow an authenticated local threat actor to bypass key commitment policy enforcement via a shared key cache, resulting in ciphertext that can be decrypted to multiple different plaintexts.

Impacted versions:

- From 2.0 to 2.5.1
- From 3.0 to 3.3.0
- From 4.0 to 4.0.4

Resolution:

This issue has been addressed in ESDK for Python versions 3.3.1 and 4.0.5. We recommend upgrading to the latest version and ensuring any forked or derivative code is patched to incorporate the new fixes.

Workarounds:

If a customer requires operating m
key commitment policies, they mu

References:

- CVE-2026-6550
- GHSA-v638-38fc-rhfv

Acknowledgement:

We would like to thank 1seal.org for collaborating on this issue through the coordinated vulnerabili
disclosure process.

Please email aws-security@amazon.com with any security questions or concerns.