

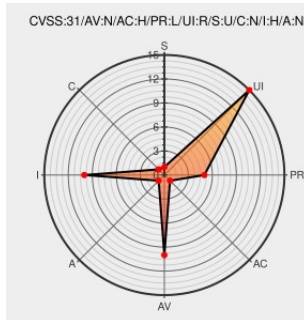


CVE-2020-8897

Published on: 11/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:59 PM UTC

CVE-2020-8897

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Aws Encryption Sdk](#) from [Amazon](#) contain the following vulnerability:

A weak robustness vulnerability exists in the AWS Encryption SDKs for Java, Python, C and Javalcript prior to versions 2.0.0. Due to the non-committing property of AES-GCM (and other AEAD ciphers such as AES-GCM-SIV or (X)ChaCha20Poly1305) used by the SDKs to encrypt messages, an attacker can craft a unique cyphertext which will decrypt to multiple different results, and becomes especially relevant in a multi-recipient setting. We recommend users update their SDK to 2.0.0 or later.

CVE-2020-8897 has been assigned by security@google.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Amazon - AWS SDK** version < 2.0.0

CVSS3 Score: **8.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: **5.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Improved client-side encryption: Explicit KeyIds and key commitment AWS Security Blog	Vendor Advisory aws.amazon.com text/html	 CONFIRM aws.amazon.com/blogs/security/improved-client-side-encryption-explicit-keyids-and-key-commitment/
AWS: In-band protocol negotiation and robustness weaknesses in AWS KMS and Encryption SDKs · Advisory · google/security-research · GitHub	Exploit Mitigation Third Party Advisory github.com text/html	 CONFIRM github.com/google/security-research/security/advisories/GHSA-wqgp-vphw-hphf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

- [980453](#) Python (pip) Security Update for aws-encryption-sdk (GHSA-wqgp-vphw-hphf)
- [980454](#) Java (maven) Security Update for com.amazonaws:aws-encryption-sdk-java (GHSA-wqgp-vphw-hphf)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Amazon	Aws Encryption Sdk	All	All	All	All
Application	Amazon	Aws Encryption Sdk	All	All	All	All
cpe:2.3:a:amazon:aws_encryption_sdk:*****:						
cpe:2.3:a:amazon:aws_encryption_sdk:*****:						

Discovery Credit

Thai Duong

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

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