

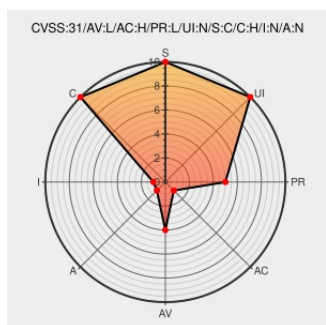


CVE-2020-8911

Published on: 08/11/2020 12:00:00 AM UTC

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

CVE-2020-8911

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

Certain versions of [Aws S3 Crypto Sdk](#) from [Amazon](#) contain the following vulnerability:

A padding oracle vulnerability exists in the AWS S3 Crypto SDK for GoLang versions prior to V2. The SDK allows users to encrypt files with AES-CBC without computing a Message Authentication Code (MAC), which then allows an attacker who has write access to the target's S3 bucket and can observe whether or not an endpoint with

access to the key can decrypt a file, they can reconstruct the plaintext with (on average) 128*length (plaintext) queries to the endpoint, by exploiting CBC's ability to manipulate the bytes of the next block and PKCS5 padding errors. It is recommended to update your SDK to V2 or later, and re-encrypt your files.

CVE-2020-8911 has been assigned by security@google.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: Google LLC - AWS S3 Crypto SDK for GoLang version <= V1

CVSS3 Score: **5.6 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	NONE	NONE

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
CBC padding oracle issue in AWS S3 Crypto SDK for golang · Advisory · google/security-research · GitHub	Exploit Third Party Advisory github.com text/html	 CONFIRM github.com/google/security-research/security/advisories/GHSA-f5pg-7wfw-84q9
Updates to the Amazon S3 Encryption Client AWS Developer Blog	Vendor Advisory aws.amazon.com text/html	 CONFIRM aws.amazon.com/blogs/developer/updates-to-the-amazon-s3-encryption-client/?s=09

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Amazon	Aws S3 Crypto Sdk	All	All	All	All
Application	Amazon	Aws S3 Crypto Sdk	All	All	All	All
cpe:2.3:a:amazon:aws_s3_crypto_sdk:*:*:*:*:golang:*:*						
cpe:2.3:a:amazon:aws_s3_crypto_sdk:*:*:*:*:golang:*:*						

Discovery Credit

Sophie Schmieg

Social Mentions

Source	Title	Posted (UTC)
 @tomtwinklestar	aws-sdk-go v1からv2への切り替えモニョモニョしている間にCVE-2020-8911,CVE-2020-8912が来てバタバタv2に切り替えた 取り敢えずヨシ！	2022-09-02 10:26:16

[← 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](#)