

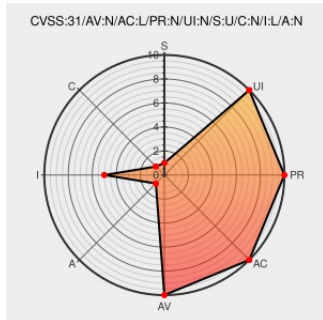


CVE-2020-8929

Published on: 10/19/2020 12:00:00 AM UTC

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

CVE-2020-8929

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

Certain versions of [Tink](#) from [Google](#) contain the following vulnerability:

A mis-handling of invalid unicode characters in the Java implementation of Tink versions prior to 1.5 allows an attacker to change the ID part of a ciphertext, which result in the creation of a second ciphertext that can decrypt to the same plaintext. This can be a problem with encrypting deterministic AEAD with a single key, and rely on a unique ciphertext-per-plaintext.

CVE-2020-8929 has been assigned by [Google](#) security@google.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Google LLC](#) - **Tink** version < 1.5

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Fixing ciphertext malleability issue	Patch	CONFIRM

in Java caused by storing the ci... ·
google/tink@93d839a · GitHub

Third Party Advisory

github.com

text/html

github.com/google/tink/commit/93d839a5865b9d950dffdc9d0bc99b71280a8899

Ciphertext Malleability Issue in Tink
Java · Advisory · google/tink ·
GitHub

Patch

Third Party Advisory

github.com

text/html

CONFIRM github.com/google/tink/security/advisories/GHSA-g5vf-v6wf-7w2r

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

983214 Java (maven) Security Update for com.google.crypto.tink:tink (GHSA-g5vf-v6wf-7w2r)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tink	All	All	All	All
Application	Google	Tink	All	All	All	All
cpe:2.3:a:google:tink:*****:						
cpe:2.3:a:google:tink:*****:						

Discovery Credit

Peter Esbensen