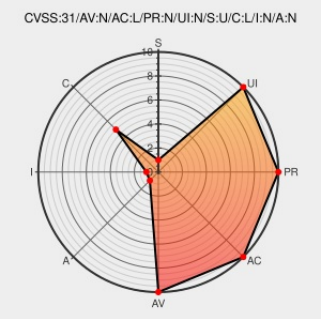
CVE-2021-37606

Published on: 07/28/2021 12:00:00 AM UTC

Last Modified on: 08/08/2023 02:22:00 PM UTC

CVE-2021-37606

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Meow Hash from Meow Hash Project contain the following vulnerability:

Meow hash 0.5/calico does not sufficiently thwart key recovery by an attacker who can query whether there's a collision in the bottom bits of the hashes of two messages, as demonstrated by an attack against a long-running web service that allows the attacker to infer collisions by measuring timing differences.

CVE-2021-37606 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

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	LOW	NONE	NONE

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Cryptanalysis of Meow Hash | Hacker News	news.ycombinator.com text/html	MISC news.ycombinator.com/item?id=27978878
Cryptanalysis of Meow Hash | Content	peter.website	MISC peter.website/meow-hash-cryptanalysis

Cryptanalysis of Meow Hash | Content peter.website text/html MISC peter.website/meow-hash-cryptanalysis

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	Meow Hash Project	Meow Hash	0.5	All	All	All

cpe:2.3:a:meow_hash_project:meow_hash:0.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-37606 : Meow hash 0.5/calico does not sufficiently thwart key recovery by an attacker who can query whethe… twitter.com/i/web/status/1…	2021-07-28 19:45:24
@LinInfoSec	Calico - CVE-2021-37606: peter.website/meow-hash-cryp…	2021-07-30 16:35:11

← Previous ID Next ID→