



CVE-2021-41168

Published on: 10/21/2021 12:00:00 AM UTC

Last Modified on: 07/17/2023 03:17:00 PM UTC

CVE-2021-41168 - advisory for GHSA-6gvv-9q92-w5f6

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

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Snudown](#) from [Reddit](#) contain the following vulnerability:

Snudown is a reddit-specific fork of the Sundown Markdown parser used by GitHub, with Python integration added. In affected versions snudown was found to be vulnerable to denial of service attacks to its reference table implementation. References written in markdown `[reference\_name]: https://www.example.com` are inserted into a hash

table which was found to have a weak hash function, meaning that an attacker can reliably generate a large number of collisions for it. This makes the hash table vulnerable to a hash-collision DoS attack, a type of algorithmic complexity attack. Further the hash table allowed for duplicate entries resulting in long retrieval times. Proofs of concept and further discussion of the hash collision issue are discussed on the snudown GHSA(<https://github.com/reddit/snudown/security/advisories/GHSA-6gvv-9q92-w5f6>). Users are advised to update to version 1.7.0.

CVE-2021-41168 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **reddit** - **snudown** version < 1.7.0

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

Hash-collision denial-of-service vulnerabilities (#87) · reddit/snudown@1ac2c13 · GitHub

github.com

text/html

MISC

github.com/reddit/snudown/commit/1ac2c130b210539ee1e5d67a7bac93f9d8007c0e

Hash-Collision Denial-of-Service Vulnerability in Reference Table · Advisory · reddit/snudown · GitHub

github.com

text/html

CONFIRM

github.com/reddit/snudown/security/advisories/GHSA-6gvv-9q92-w5f6

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

Reddit

Snudown

All

All

All

All

cpe:2.3:a:reddit:snudown:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source

Title

Posted (UTC)

@CVEreport

CVE-2021-41168 : Snudown is a reddit-specific fork of the Sundown Markdown parser used by GitHub, with Python integ... twitter.com/i/web/status/1...

2021-10-21 20:16:09

@LinInfoSec

Python - CVE-2021-41168: github.com/reddit/snudown...

2021-10-28 05:51:40

← Previous ID

Next ID →

