



CVE-2021-21387

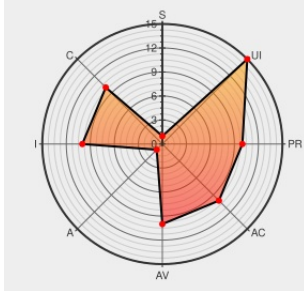
Published on: 03/19/2021 12:00:00 AM UTC

Last Modified on: 03/25/2021 07:35:00 PM UTC

CVE-2021-21387 - advisory for GHSA-5jxh-6378-rg7v

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

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



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

Wrongthink peer-to-peer, end-to-end encrypted messenger with PeerJS and Axolotl ratchet. In wrongthink from version 2.0.0 and before 2.3.0 there was a set of vulnerabilities causing inadequate encryption strength. Part of the secret identity key was disclosed by the fingerprint used for connection. Additionally, the safety number was

improperly calculated. It was computed using part of one of the public identity keys instead of being derived from both public identity keys. This caused issues in computing safety numbers which would potentially be exploitable in the real world. Additionally there was inadequate encryption strength due to use of 1024-bit DSA keys. These issues are all fixed in version 2.3.0.

CVE-2021-21387 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [parabirb](#) - **wrongthink** version $\geq 2.0.0$, $< 2.2.0$

CVSS3 Score: **7.5 - HIGH**

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

Partial secret key disclosure, improper safety number calculation, & inadequate encryption strength · Advisory · parabirb/wrongthink · GitHub

[github.com](#)
[text/html](#)

 CONFIRM
github.com/parabirb/wrongthink/security/advisories/GHSA-5jxh-6378-rg7v

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	Wrongthink	Wrongthink	All	All	All	All
-------------	----------------------------	----------------------------	-----	-----	-----	-----

cpe:2.3:a:wrongthink:wrongthink:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← 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](#)