

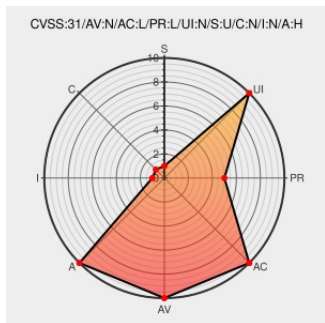


CVE-2021-32666

Published on: 06/03/2021 12:00:00 AM UTC

Last Modified on: 06/11/2021 07:33:00 PM UTC

CVE-2021-32666 - advisory for GHSA-2x9x-vh27-h4rv

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

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

wire-ios is the iOS version of Wire, an open-source secure messaging app. In wire-ios versions 3.8.0 and prior, a vulnerability exists that can cause a denial of service between users. If a user has an invalid assetID for their profile picture and it contains the " character, it will cause the iOS client to crash. The vulnerability is patched in wire-ios version 3.8.1.

CVE-2021-32666 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [wireapp](#) - wire-ios version <= 3.8.0

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
-------------	------	------

Merge pull request from GHSA-789p-78mj-hfmc · wireapp/wire-ios-data-model@35af3f6 · GitHub

github.com

text/html

MISC github.com/wireapp/wire-ios-data-model/commit/35af3f632085f51a2ce7f608fdaeffd1a69ad89f

Asset DoS vulnerability · Advisory · wireapp/wire-ios · GitHub

github.com

text/html

CONFIRM github.com/wireapp/wire-ios/security/advisories/GHSA-2x9x-vh27-h4rv

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	Wire	Wire	All	All	All	All

cpe:2.3:a:wire:wire:*:*:*:*:*:iphone_os:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32666 : wire-ios is the iOS version of Wire, an open-source secure messaging app. In wire-ios versions 3.8... twitter.com/i/web/status/1...	2021-06-03 21:38:36
@SecRiskRptSME	RT: CVE-2021-32666 wire-ios is the iOS version of Wire, an open-source secure messaging app. In wire-ios versions... twitter.com/i/web/status/1...	2021-06-04 07:36:59
/r/netcve	CVE-2021-32666	2021-06-03 22:41:09

← Previous ID

Next ID →