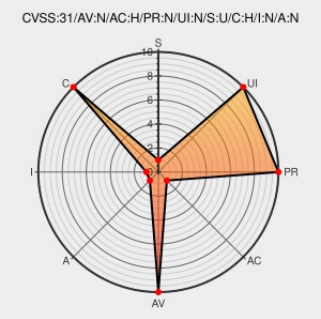
# CVE-2023-33982

Published on: Not Yet Published

Last Modified on: 06/01/2023 03:55:00 PM UTC

## CVE-2023-33982

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




Certain versions of Briar from Briarproject contain the following vulnerability:

Bramble Handshake Protocol (BHP) in Briar before 1.5.3 is not forward secure: eavesdroppers can decrypt network traffic between two accounts if they later compromise both accounts. NOTE: the eavesdropping is typically impractical because BHP runs over an encrypted session that uses the Tor hidden service protocol.

CVE-2023-33982 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 5.9 - MEDIUM

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

### CVE References

| Description | Tags | Link |
|---|---|---|
| | ethz.ch application/pdf | MISC ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/appliedcrypto/education/theses/report_YuanmingSong.pdf |
| Three security issues found and fixed - Briar | briarproject.org text/html | MISC briarproject.org/news/2023-three-security-issues-found-and-fixed/ |

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 | Briarproject | Briar | All | All | All | All |

cpe:2.3:a:briarproject:briar:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→