

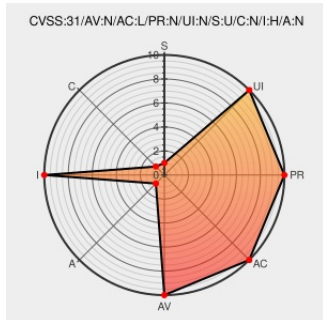


CVE-2019-13000

Published on: 01/31/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:46 PM UTC

CVE-2019-13000

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

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

Eclair through 0.3 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "it is beta-quality software and don't put too much money in it."

CVE-2019-13000 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

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	NONE	HIGH	NONE

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Commits · ACINQ/eclair · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/ACINQ/eclair/commits/master

Releases · ACINQ/eclair · GitHub

Release Notes

Third Party Advisory

github.com

text/html

MISC github.com/ACINQ/eclair/releases

[Lightning-dev] Full Disclosure: CVE-2019-12998 / CVE-2019-12999 / CVE-2019-13000

Exploit

Mailing List

Third Party Advisory

lists.linuxfoundation.org

text/html

CONFIRM

lists.linuxfoundation.org/pipermail/lightning-dev/2019-September/002174.html

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

Exploit/POC from Github

A tool that detect if your node has been victim of the invalid funding tx attack.

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Acinq	Eclair	All	All	All	All
cpe:2.3:a:acinq:eclair:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →