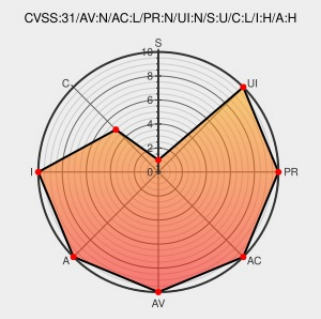
CVE-2021-41592

Published on: 10/04/2021 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-41592

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



Certain versions of C-lightning from Elementsproject contain the following vulnerability:

Blockstream c-lightning through 0.10.1 allows loss of funds because of dust HTLC exposure.

CVE-2021-41592 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.4 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
[Lightning-dev] Full Disclosure: CVE-2021-41591/ CVE-2021-41592 / CVE-2021-41593 "Dust HTLC Exposure Considered Harmful"	lists.linuxfoundation.org text/html	MISC lists.linuxfoundation.org/pipermail/lightning-dev/2021-October/003264.html
GitHub - ElementsProject/lightning: c-lightning — a Lightning	github.com	MISC

Network implementation in C	text/html	github.com/ElementsProject/lightning
Lightning Network Griefing Attacks %%page%% %%sep%% %%sitename%% - Bitcoin Magazine: Bitcoin News, Articles, Charts, and Guides	bitcoinmagazine.com text/html	MISC bitcoinmagazine.com/technical/good-griefing-a-lingering-vulnerability-on-lightning-network-that-still-needs-fixing
[Lightning-dev] Miners Dust Inflation attacks on Lightning Network	lists.linuxfoundation.org text/html	MISC lists.linuxfoundation.org/pipermail/lightning-dev/2020-May/002714.html
[Lightning-dev] Full Disclosure: CVE-2021-41591/ CVE-2021-41592 / CVE-2021-41593 "Dust HTLC Exposure Considered Harmful"	lists.linuxfoundation.org text/html	MISC lists.linuxfoundation.org/pipermail/lightning-dev/2021-October/003257.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elementsproject	C-lightning	All	All	All	All

cpe:2.3:a:elementsproject:c-lightning:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@miketwenty1	Please update your LND nodes to v0.13.3-beta github.com/lightningnetwo… This fixes a vulnerability - CVE-2021-41592	2021-10-04 16:38:21
@CVEreport	CVE-2021-41592 : Blockstream c-lightning through 0.10.1 allows loss of funds because of dust HTLC exposure.... cve.report/CVE-2021-41592	2021-10-04 17:10:19
@LinInfoSec	Lightning - CVE-2021-41592: lists.linuxfoundation.org/pipermail/ligh…	2021-10-04 19:15:18
@bCyberBasti	@BtcpayServer is there an ETA for Updates regarding CVE-2021-41591 CVE-2021-41592 and CVE-2021-41593 ?	2021-10-04 22:21:13
@modrobert	[Lightning-dev] Full Disclosure: CVE-2021-41591/ CVE-2021-41592 / CVE-2021-41593 "Dust HTLC Exposure Considered Har… twitter.com/i/web/status/1…	2021-10-04 22:31:29
@CarlosMelzer	In the actual case of vulnerability (CVE-2021-41592) please update your Raspiblitz LND to the actual patched vers… twitter.com/i/web/status/1…	2021-10-05 04:22:28
@nobsbitcoin	[Lightning-dev] Full Disclosure: CVE-2021-41591/ CVE-2021-41592 / CVE-2021-41593 "Dust HTLC Exposure Considered Har… twitter.com/i/web/status/1…	2021-10-06 12:43:07
/r/raspibolt	⚠ Important security update: upgrade LND to v0.13.3! ⚠	2021-10-04 17:25:23

← Previous ID Next ID→

CVE.report and Source URL Uptime Status status.cve.report