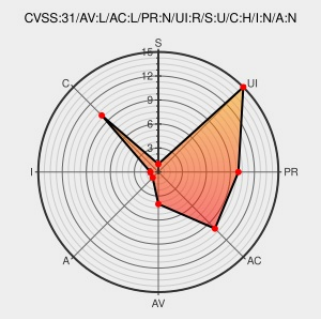
CVE-2022-31246

Published on: Not Yet Published

Last Modified on: 06/28/2022 02:12:00 PM UTC

CVE-2022-31246

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



Certain versions of Electrum from Electrum contain the following vulnerability:

paymentrequest.py in Electrum before 4.2.2 allows a file:// URL in the r parameter of a payment request (e.g., within QR code data). On Windows, this can lead to capture of credentials over SMB. On Linux and UNIX, it can lead to a denial of service by specifying the /dev/zero filename.

CVE-2022-31246 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
BIP70 payment requests `?r=` field supports `file://` URIs, allowing attacker to trick victim machine to `open()` arbitrary file · Advisory · spesmilo/electrum · GitHub	github.com text/html	MISC github.com/spesmilo/electrum/security/advisories/GHSA-4fh4-hx35-r355

Electrum on Twitter: "Electrum 4.2.2 fixes a vulnerability that can be exploited on some Windows+SMB configurations. Please upgrade if you have not done so already. More details here: https://t.co/xn2bWQQkIZ"	nitter.domain.glass text/html	MISC twitter.com/ElectrumWallet/status/1534540879905665028

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Electrum	Electrum	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

cpe:2.3:a:electrum:electrum:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31246 : paymentrequest.py in Electrum before 4.2.2 allows a file:// URL in the r parameter of a paym… twitter.com/i/web/status/1…	2022-06-17 14:04:33
/r/Namecoin	Electrum-NMC v4.0.0b1 and ncdns v0.3.1 fix CVE-2022-31246 -- Patch Your Systems Now!	2022-06-08 22:13:58
/r/netcve	CVE-2022-31246	2022-06-17 14:38:11

← Previous ID

Next ID→