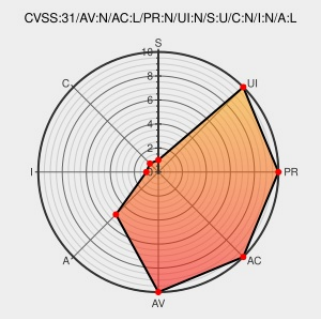
CVE-2020-12439

Published on: 05/05/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:35 PM UTC

CVE-2020-12439

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



Certain versions of Grin from Grin contain the following vulnerability:

Grin before 3.1.0 allows attackers to adversely affect availability of data on a Mimblewimble blockchain.

CVE-2020-12439 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Rework output_pos index (better txhashset transactional support) · Issue #3235 · mimblewimble/grin · GitHub	Issue Tracking, Patch, Third Party Advisory, github.com, text/html	CONFIRM github.com/mimblewimble/grin/issues/3235

Block input bitmap rework by antiochp · Pull Request #3236 · mimblewimble/grin · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/mimblewimble/grin/pull/3236
grin-security/CVE-2020-12439.md at master · mimblewimble/grin-security · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/mimblewimble/grin-security/blob/master/CVEs/CVE-2020-12439.md

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Grin	Grin	All	All	All	All
Application	Grin	Grin	All	All	All	All

cpe:2.3:a:grin:grin:*:*:*:*:*:*:*:*:

cpe:2.3:a:grin:grin:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→