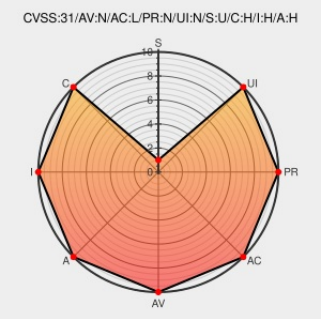
CVE-2019-9195

Published on: 02/26/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:08 PM UTC

CVE-2019-9195

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



Certain versions of Grin from Grin contain the following vulnerability:

util/src/zip.rs in Grin before 1.0.2 mishandles suspicious files. An attacker can execute arbitrary code via directory traversal in a ZIP archive.

CVE-2019-9195 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	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
Don't extract unexpected files from txhashset archive by hashmap · Pull Request #2624 · mimblewimble/grin · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/mimblewimble/grin/pull/2624

Release v1.0.2 · mimblewimble/grin · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/mimblewimble/grin/releases/tag/v1.0.2
No Description Provided	Exploit Issue Tracking Third Party Advisory www.grin-forum.org text/html	MISC www.grin-forum.org/t/critical-vulnerability-in-grin-1-0-1-and-older-fixed-in-1-0-2/4343

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

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→