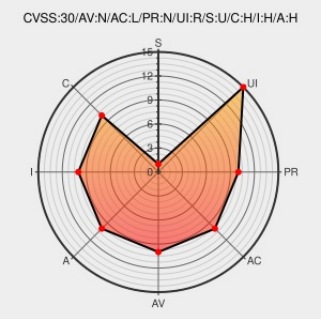
CVE-2018-1000093

Published on: 03/13/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:30 PM UTC

CVE-2018-1000093

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



Certain versions of Cryptonote from Cryptonote contain the following vulnerability:

CryptoNote version version 0.8.9 and possibly later contain a local RPC server which does not require authentication, as a result the walletd and the simplewallet RPC daemons will process any commands sent to them, resulting in remote command execution and a takeover of the cryptocurrency wallet if an attacker can trick an application such as a web browser into connecting and sending a command for example. This attack appears to be exploitable via a victim visiting a webpage hosting malicious content that trigger such behavior.

CVE-2018-1000093 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link

Unauthenticated JSON-RPC API allows takeover of CryptoNote RPC wallets | Ayrx's Blog	Exploit Third Party Advisory www.ayrx.me text/html	MISC www.ayrx.me/cryptonote-unauthenticated-json-rpc
	Broken Link Third Party Advisory github.com text/plain Inactive Link Not Archived	MISC github.com/amjuarez/bytecoin/issues/217
Unauthenticated JSON-RPC API allows takeover of CryptoNote RPC wallets · Issue #172 · cryptonotefoundation/cryptonote · GitHub	Exploit Issue Tracking Third Party Advisory github.com text/html	MISC github.com/cryptonotefoundation/cryptonote/issues/172

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

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:cryptonote:cryptonote:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→