

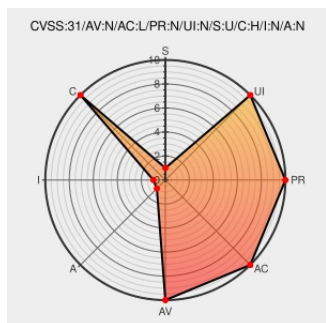


CVE-2013-10006

Published on: Not Yet Published

Last Modified on: 10/12/2023 09:15:00 AM UTC

CVE-2013-10006

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Primecoin](#) from [Ziftrshop](#) contain the following vulnerability:

A vulnerability classified as problematic was found in Ziftr primecoin up to 0.8.4rc1. Affected by this vulnerability is the function HTTPAuthorized of the file src/bitcoinrpc.cpp. The manipulation of the argument strUserPass/strRPCUserColonPass leads to observable timing discrepancy. The complexity of an attack is rather high. The

exploitation appears to be difficult. Upgrading to version 0.8.4rc2 is able to address this issue. The patch is named cdb3441b5cd2c1bae49fae671dc4a496f7c96322. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217171.

CVE-2013-10006 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Ziftr** - **primecoin** version = **0.8.4rc1**

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
CVE-2013-10006 Ziftr primecoin bitcoinrpc.cpp HTTPAuthorized timing discrepancy	vuldb.com text/html	MISC vuldb.com/?ctiid.217171
Release v0.8.4rc2 - Ziftr/primecoin - GitHub	github.com text/html	MISC github.com/Ziftr/primecoin/releases/tag/v0.8.4rc2
CVE-2013-10006 Ziftr primecoin	vuldb.com	MISC vuldb.com/?id.217171

bitcoinrpc.cpp HTTPAuthorized timing discrepancy

text/html

Make RPC password resistant to timing attacks · Ziftr/primecoin@cdb3441 · GitHub

github.com

text/html

MISCgithub.com/Ziftr/primecoin/commit/cdb3441b5cd2c1bae49fae671dc4a496f7c96322

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	Ziftrshop	Primecoin	All	All	All	All
Application	Ziftrshop	Primecoin	0.8.4	rc1	All	All

cpe:2.3:a:ziftrshop:primecoin:*****:

cpe:2.3:a:ziftrshop:primecoin:0.8.4:rc1:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→