



# CVE-2022-36111

Published on: Not Yet Published

Last Modified on: 11/27/2022 04:33:00 AM UTC

## CVE-2022-36111 - advisory for GHSA-672p-m5jq-mrh8

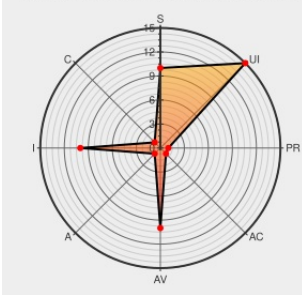
[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:N



Certain versions of [Immudb](#) from [Codenotary](#) contain the following vulnerability:

immudb is a database with built-in cryptographic proof and verification. In versions prior to 1.4.1, a malicious immudb server can provide a falsified proof that will be accepted by the client SDK signing a falsified transaction replacing the genuine one. This situation can not be triggered by a genuine immudb server and requires the client to

perform a specific list of verified operations resulting in acceptance of an invalid state value. This vulnerability only affects immudb client SDKs, the immudb server itself is not affected by this vulnerability. This issue has been patched in version 1.4.1.

CVE-2022-36111 has been assigned by [security-advisories@github.com](mailto:security-advisories@github.com) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **codenotary** - **immudb** version < 1.4.1

CVSS3 Score: **5.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>HIGH</b>	<b>NONE</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>NONE</b>	<b>HIGH</b>	<b>NONE</b>

### CVE References

Description	Tags	Link
Release v1.4.1 · codenotary/immudb · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/codenotary/immudb/releases/tag/v1.4.1">github.com/codenotary/immudb/releases/tag/v1.4.1</a>
client package - github.com/codenotary/immudb/pkg/client - pkg.go.dev	<a href="#">pkg.go.dev</a> <a href="#">text/html</a>	MISC <a href="https://pkg.go.dev/github.com/codenotary/immudb/pkg/client">pkg.go.dev/github.com/codenotary/immudb/pkg/client</a>

immudb/docs/security/vulnerabilities/linear-fake at master · codenotary/immudb · GitHub

github.com  
text/html

MISC

github.com/codenotary/immudb/tree/master/docs/security/vulnerabilities/linear-fake

Insufficient Verification of Proofs generated by the immudb server in client SDK. · Advisory · codenotary/immudb · GitHub

github.com  
text/html

CONFIRM m5jq-mrh8

github.com/codenotary/immudb/security/advisories/GHSA-672p-m5jq-mrh8

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](mailto: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	Codenotary	Immudb	All	All	All	All
cpe:2.3:a:codenotary:immudb:*****:						

No vendor comments have been submitted for this CVE

### Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	<a href="#">CVE-2022-36111</a>	2022-11-23 18:38:33

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)