



nimiq-block has skip block quorum bypass via out-of-range BitSet indices & u16 truncation

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-33471
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 20:16:40 UTC
Updated	2026-04-22 21:23:52 UTC
Description	nimiq-block contains block primitives to be used in Nimiq's Rust implementation. `SkipBlockProof::verify` computes its quorum

Risk And Classification

Primary CVSS: v3.1 9.6 CRITICAL from security-advisories@github.com

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H

Problem Types: CWE-20 | CWE-190 | CWE-345 | CWE-1284 | CWE-20 CWE-20: Improper Input Validation | CWE-190 CWE-190: Integer Overflow or Wraparound | CWE-345 CWE-345: Insufficient Verification of Data Authenticity | CWE-1284 CWE-1284: Improper Validation of Specified Quantity in Input

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H
3.1	CNA	DECLARED	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Confidentiality

None

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Nimiq	Nimiq-block	affected < 1.3.0	Not specified

References

Reference	Source	Link	Tags
github.com/nimiq/core-rs-albatross/releases/tag/v1.3.0	security-advisories@github.com	github.com	
github.com/nimiq/core-rs-albatross/commit/d02059053181ed8ddad6b59a0adfd6...	security-advisories@github.com	github.com	
github.com/nimiq/core-rs-albatross/security/advisories/GHSA-6973-8887-87ff	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report