

nimiq / **core-rs-albatross** Public[Code](#) [Issues](#) 85 [Pull requests](#) 35 [Actions](#) [Projects](#) [Security and quality](#)

Panic via RequestMacroChain micro-block locator

Moderate jsdanielh published **GHSA-48m6-486p-9j8p** 3 days ago

Package

nimiq-consensus (Rust)

Affected versions

<=v1.2.2

Patched versions

v1.3.0

Description

Impact

An unauthenticated p2p peer can cause the `RequestMacroChain` message handler task to panic by sending a `RequestMacroChain` message where the first locator hash that is on the victim's main chain is a micro block hash (not a macro block hash).

In `RequestMacroChain::handle`, the handler selects the locator based only on "is on main chain", then calls `get_macro_blocks()` and panics via `.unwrap()` when the selected hash is not a macro block (`BlockchainError::BlockIsNotMacro`).

Patches

The patch for this vulnerability([#3660](#)) is formally released as part of [v1.3.0](#).

Workarounds

No known workarounds.

References

See [PR](#).

Severity

Moderate 5.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	Low

[Learn more about base metrics](#)

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

CVE ID

CVE-2026-34069

Weaknesses

▶ CWE-617

Credits

 jsdanielh

Analyst

 1seal

Finder