

nimiq / core-rs-albatross Public

<> Code Issues 85 Pull requests 32 Actions Projects Security and qua

Fix discovery handler underflow when peer sends limit=0 #3664

Closed jsdanielh wants to merge 0 commit into albatross from fix/discovery-handler-limit-underflow

Conversation 1 Commits 0 Checks 0 Files changed 0

jsdanielh commented last week Member

Summary

- A peer sending `limit=0` during the discovery handshake caused an underflow in the periodic update path where `peer_list_limit - 1` wraps to `usize::MAX`, triggering a capacity overflow panic.
- Clamp the peer-supplied limit to our own `update_limit` on receipt, and use `saturating_sub(1)` when computing the update list size.

viquezclaudio approved these changes last week

[View reviewed changes](#)

jsdanielh closed this last week

jsdanielh force-pushed the fix/discovery-handler-limit-underflow branch from 699597d to 8f60a2d last week [Compare](#)

jsdanielh commented last week Member Author

Merged into albatross : 8f60a2d

Sign up for free

to join this conversation on GitHub. Already have an account? [Sign in to](#)

[comment](#)

Reviewers



viquezclaudio



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants

