

nimiq / **core-rs-albatross** Public[Code](#) [Issues](#) 85 [Pull requests](#) 32 [Actions](#) [Projects](#) [Security and quality](#)

# Discovery handshake limit could underflow and later provoke a deterministic overflow panic

**High** jsdanielh published GHSA-5rm9-893q-vmhm 4 days ago

## Package

**nimiq-network-libp2p** (Rust)

### Affected versions

&lt;=v1.2.2

### Patched versions

v1.3.0

## Description

### Impact

The discovery handler accepts a peer-controlled limit during handshake and stores it unchanged. The immediate `HandshakeAck` path then honors `limit = 0` and returns zero contacts, which makes the session look benign.

Later, after the same session reaches `Established`, the periodic update path computes `self.peer_list_limit.unwrap()` as `usize - 1`. With `limit = 0`, that wraps to `usize::MAX` and then in `rand 0.9.2`, `choose_multiple()` immediately attempts `Vec::with_capacity(amount)`, which deterministically panics with capacity overflow.

### Patches

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

### Workarounds

No known workarounds.

### References

See [PR](#).

### Severity

**High** 7.5 / 10

#### CVSS v3 base metrics

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

[Learn more about base metrics](#)

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

### CVE ID

CVE-2026-33184

### Weaknesses

► CWE-191

### Credits

 jsdanielh

Analyst