nimiq / **core-rs-albatross** Public

Code Issues 86 Pull requests 32 Actions Projects Security and qua

Commit `8f60a2d`

jsdanielh committed last week · 8 / 8 · Verified

```
Fix discovery handler underflow when peer sends limit=0

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.
```

albatross · v1.3.0

1 parent 44b15d1 commit 8f60a2d

1 file changed +4 -3 lines changed

Top

Filter files…

network-libp2p/src/discovery

handler.rs

1 file changed +4 -3 lines changed

Search within code

network-libp2p/src/discovery/handler.rs

```
@@ -466,8 +466,9 @@ impl ConnectionHandler for Handler {
466  466                                    let response_signature =
467  467
                        self.keypair.tagged_sign(&challenge_nonce);
468  468
469      -                                  // Remember peer's filter
470      -                                  self.peer_list_limit = Some(limit);
     469  +                                  // Remember peer's filter, clamping to our
                        own update limit
```

```
      470 +                                    self.peer_list_limit =
      471 +
          Some(limit.min(self.config.update_limit));
471   472                                      self.services_filter = services;
472   473
473   474                                      let peer_contact_book =
          self.peer_contact_book.read();
          @@ -758,7 +759,7 @@ impl ConnectionHandler for Handler {
758   759                                      let peer_contact_book =
          &self.peer_contact_book.read();
759   760                                      let mut peer_contacts =
          self.get_peer_contacts(
760   761                                          peer_contact_book,
761       -                                    self.peer_list_limit.unwrap() as usize
          - 1,
      762 +                                    (self.peer_list_limit.unwrap() as
          usize).saturating_sub(1),
762   763                                      );
763   764                                      // Always include our own contact for
          updates
764   765                                      peer_contacts
```

Comments 0

Please sign in to comment.