Learnings from the Nomad Hack

From NoMad to Very Mad

Odysseas.eth
Protocol Engineer, Nomad
I am not here on behalf of Illusory, and the views I express today are my own and do not reflect those of the company.
whoami

Worked as web3 consultant

Worked in DevOps and IoT

Blog: odyslam.com/blog

Twitter: @odysseas_eth
Agenda

- **What** is Nomad?
- **How** did the Incident happen?
- **What** suggestions do we have for protocols
Nomad is Not a Bridge
Nomad has a Bridge
Nomad is an optimistic protocol
Nomad is an optimistic protocol for interoperability
Nomad is an optimistic protocol for **interoperability** that supports **arbitrary messages** between domains.
ELI5 How Nomad works
Life Cycle of Message in Nomad

Dispatch Message, Relay Root, Prove Message, Process Message

Optimistic Window
ELI5 The Incident
Replica

R1 → T1

bytes32 => uint256

M1 → R1
M2 → R1

bytes32 => bytes32
Replica

bytes32 => uint256

bytes32 => bytes32
Restarting the Protocol is **Easy**

Restarting the Bridge is **Hard**

**Principles:**

1. Users should be able to collect funds as they are recovered
2. Recovered funds should be fairly distributed to users
Learnings
“Only a fool learns from his own mistakes. The wise man learns from the mistakes of others.”

― Otto von Bismarck
Test
Observe
Engage
Communicate
Test (🛠, 🔥)

- Unit Tests
- Property-based Tests
- Integration Tests
- Forking Tests
- Invariant Tests
  - Static analysis
  - Storage layout
Unit-tests

Input = 5

Function

Output = 25
Property-based tests

Input = x

Function

Output = x * 5
Integration tests
Forking tests

Inputs

Chain state

Function

Outputs
Invariant Tests

1. Define Invariants
2. Test Invariants

Example:

Every message that is received, must have been dispatched
Finally

Static Analysis Tools

Storage Layout Analysis

(Resource: forge-inspect.sh)
Priority

Unit Tests
Property-based Tests
Forking Tests
Audits
Storage layout

Easy with **Foundry**
U up?

It’s already too late

Observe 👁
Web 2 is mature, like Google SRE handbook

1. Start with Business Objectives
2. Define Actionable Alerts
3. Define Playbook for every Alert
4. Beware of Alert Fatigue 😴
1. Hereustics require human interpretation
2. Invariant alerts can be automated
We do not rise to the level of our expectations. We fall to the level of our training

- Archilochus
Focus

Explicit ownership

Explicit outcomes

Gameday. Gameday. Gameday

Read The Anatomy of a Good Emergency Procedure
Talk with users
Talk with legal
What the users want

Honesty. No sugar coating

Pre-approved messaging

- What are you doing now
- What do you plan doing next
First days after the incident

- Inform Legal Team
- Public Communication
- Partners Communication
- Chain Analytics Firm
- Recovery Address
- Align on Bounty
- Public Communication
First days after the incident

Public Communication

Chain Analytics Firm

Align on Bounty

Inform Legal Team

Partners Communication

Recovery Address

Public Communication
First days after the incident

- Inform Legal Team
- Public Communication
- Partners Communication
- Chain Analytics Firm
- Recovery Address
- Align on Bounty
- Public Communication
First days after the incident

1. Inform Legal Team
2. Public Communication
3. Partners Communication
4. Chain Analytics Firm
5. Align on Bounty
6. Recovery Address
7. Public Communication
First days after the incident

Inform Legal Team
Public Communication
Partners Communication
Chain Analytics Firm
Recovery Address
Align on Bounty
Public Communication
First days after the incident

1. Inform Legal Team
2. Public Communication
3. Partners Communication
4. Chain Analytics Firm
5. Recovery Address
6. Align on Bounty
7. Public Communication
First days after the incident

Inform Legal Team

Public Communication

Chain Analytics Firm

Recovery Address

Align on Bounty

Partners Communication

Public Communication
Maintenance

Public Communication

Chain Analytics Firm

Align on Bounty

Inform Legal Team

Partners Communication

Recovery Address

Public Communication
Thank you!

Odysseas.eth
Protocol Engineer, Nomad
odysseas@nomad.xyz

@odysseas_eth