What Really Failed in the Nomad Hack?

Zettyx research pass - hack post-mortem - Nomad - 2026-07-11

Dry humor disabled: users lost money here. Every claim is sourced or flagged missing. Review before publishing.

Research lens: A clean report names both the evidence and the blind spots.

1. The core decision

Nomad lost $190.00M on 2022-08-01 according to the fetched hack database. The question that matters is not only the headline number. It is what failed, and whether the same failure could happen elsewhere.

2. Why It Matters

Root cause beats amount lost. A large loss from a repeatable operational or contract mistake teaches more than a one-off headline.

3. What I Checked

- DeFiLlama /hacks - date, amount, chain, technique [high]
- Security / post-mortem source links - root cause confirmation [high]
- Exact funds returned and recovery status -> not quantified this run [missing]

4. What the Data Shows

Field	Value	Confidence
Date	2022-08-01	high
Amount lost	$190.00M	high
Chain / target	Ethereum - Nomad	high
Exploit type	Trusted Root Exploit	high
Root cause	faulty upgrade initialized trusted root to 0x00, causing messages to be treated as proven	high
Replicable?	Yes - source-linked review needed before publishing	high
Funds returned	Missing - needs manual check	missing

5. What the data can carry

The fetched post-mortem checks align on the root-cause shape: faulty upgrade initialized trusted root to 0x00, causing messages to be treated as proven. The right lesson is the failure mode, not the size of the loss. [medium]

6. What Was Handled / What Held

- The incident is present in DeFiLlama's hack database with date, chain, technique, and amount. [high]

- Post-mortem links are attached for manual review. [medium]

7. What remains unproven (the lesson)

- Bridge and upgrade logic can fail at system scale. [medium]
- If the root cause is repeatable, the same pattern matters for other teams. [medium]
- Funds-returned status is not quantified here. [missing]

8. What I Would Monitor Next

- Upgrade review process and whether upgrades get fresh audit attention.
- Default/sentinel values in proof or verification logic.
- Pause / circuit-breaker design and who can trigger it.
- Independent audit coverage of the upgrade path.

9. Working conclusion

This is a root-cause report, not a headline-loss report. The amount and technique are fetched; the causal story should stay at the confidence level supported by independent post-mortem sources. No jokes, no blame, no price angle. [medium]

10. Connection Use (internal)

- Reply to: bridge-security and audit threads; upgrade-safety discussions.
- Helps contact: security firms, bridge teams, audit tooling builders.
- Short reply to extract: "Root cause > amount lost."
- DM angle: upgrade-path review framing.
- $100 pack: "root-cause, not headline" post-mortem template per incident.

Missing-data checklist

[ ] Exact funds-returned figure + final net loss - verify

[ ] Timeline of white-hat vs malicious withdrawals

[ ] Protocol's own official post-mortem link

[ ] Current status of recovery / legal proceedings

Confidence notes

- Date, amount, chain, and technique: high when fetched from DeFiLlama.
- Root cause: high based on source-link checks; manually review before publishing.
- Funds-returned amount: missing unless fetched.

Sources

- https://api.llama.fi/hacks
- https://immunefi.com/blog/bug-fix-reviews/hack-analysis-nomad-bridge-august-2022/; https://www.halborn.com/blog/post/explained-the-nomad-hack-august-2022; https://cloud.google.com/blog/topics/threat-intelligence/dissecting-nomad-bridge-hack; https://www.coinbase.com/blog/nomad-bridge-incident-analysis