# THE UNASSESSED ATTACK SURFACE: Channel-Based Provenance in HPC and Quantum-Computing Open-Source Software

***When an AI agent trusts a package by its README and its Discord, who verifies the channel?***


**Pengyin Shan**
**Senior Research Software Engineer**
**National Center for Supercomputing Applications**
**University of Illinois Urbana-Champaign**
**2025–2026 Trusted CI Fellow · NSF Cybersecurity Center of Excellence**


## 01 ATTACKERS FOUND THIS LAYER FIRST

**MAR 2024**
**XZ Utils backdoor · CVE-2024-3094**
A sock-puppet pressure campaign on the project mailing list installed the attacker as co-maintainer. The channel itself was the vector [1].

**SEP–NOV 2025**
**Shai-Hulud npm worms**
Phished maintainer credentials. 1,000+ packages compromised across two waves, drawing a CISA alert [2]-[5].

**JAN 2026**
**react-codeshift**
A hallucinated package name spread to 237 repositories from one commit of 47 unreviewed LLM-generated agent files. Agents kept downloading it after registration [6].

**MAY 2026**
**Cross-ecosystem spread**
The Shai-Hulud family reached PyPI [7].

**19.7%**

**of 2.23 million packages recommended by 16 code-generating LLMs did not exist.**

43% of those hallucinations recurred on every re-run.

**Agents don't read your Git history.**
**They read your channels.**

Spracklen et al. · USENIX Security 2025 [8]

**DATASET** doi.org/10.5281/zenodo.21443211
**TOOLKIT** github.com/pengyin-shan/provenance-audit
**SUPPLEMENT** Companion demand-side audit: arXiv:2609.07754
**REFERENCES** SC26-Poster-Bibliography.bib

## 02 THE MARCH STOPS AT THE CHANNEL

| | | |
|---|---|---|
| REPOSITORY | OpenSSF Scorecard [9] | covered |
| BUILD | SLSA [10] | covered |
| ARTIFACT | Sigstore [11] | covered |
| PUBLICATION | Trusted Publishers · pnpm no-downgrade [12]-[13] | covered |
| CHANNELS | No Deployed Tool | This Work |

To our knowledge, the first framework to assess the off-repository channel layer of OSS provenance.

## 03 CHANNEL-BASED PROVENANCE · 18 SIGNALS

**How we scored:** repository, releases, documentation site, README-linked pages.

◆ 9 automated, scored for all 87 projects ○ 9 judgment-dependent, hand-verified on a stratified 30-project panel

**IDENTITY & ACCESS**

- ○ Multiple Maintainers 30/30
- ○ Admin MFA ?/30
- ◆ Admin Succession 0/30
- ◆ Contributing Guide 62%
- ◆ Governance Doc 1/87

**COMMUNICATION CHANNELS**

- ◆ Channels Declared 75%
- ◆ Channels Documented 75%
- ○ Official-channel Statement 22/30
- ○ Impersonation Reporting 0/30

**KNOWLEDGE INFRASTRUCTURE**

- ◆ Security Policy 25%
- ○ Disclosure Depth 7/3/20
- ◆ CHANGELOG 21%
- ◆ Release Notes 94%

**DISTRIBUTION METADATA**

- ◆ Stable Releases 94%
- ◆ Archival DOI 20%
- ○ Signed Releases 2/30
- ○ SBOM 0/30
- ○ Attestation 1/30

## 04 THE VERDICT, HAND-VERIFIED (N = 30)

**0** of 30 — **IMPERSONATION REPORTING**
A fake account, channel, or package has nowhere to be reported.

**0** of 30 — **ADMIN SUCCESSION**
When a maintainer leaves, nobody is named to own the channel.

**0** of 30 — **SBOM**
"Are we affected?" means digging through the code by hand.

**2** of 30 — **SIGNED RELEASES**
A hijacked account ships artifacts nobody can tell apart.

**1** of 30 — **ATTESTATION**
Downgrade blocking has almost nothing to check against.

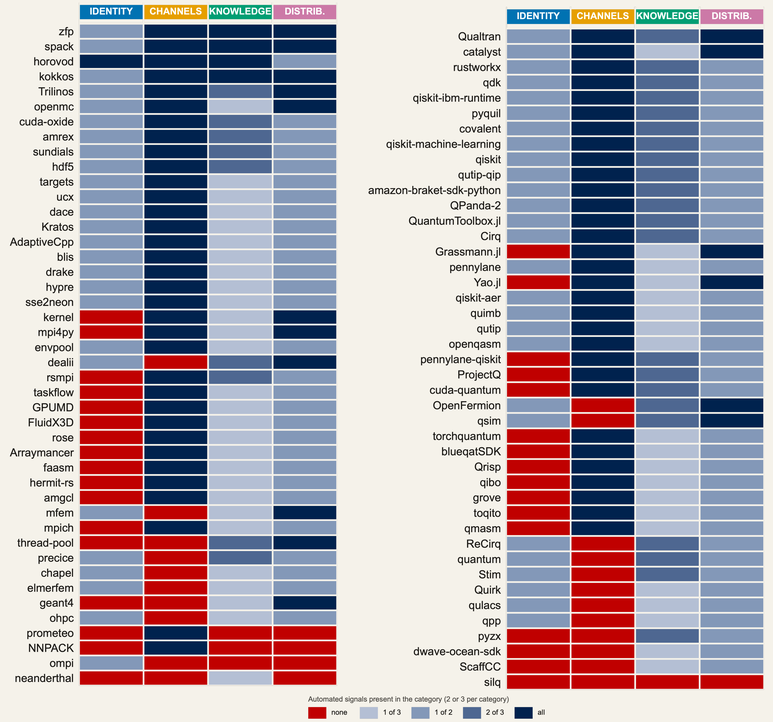
***The controls catching the next XZ are essentially NOT deployed in HPC & QC open source.***

## 05 THE PROVENANCE LAYER IS NEARLY ABSENT

Both domains look alike: channels get declared, and identity and knowledge controls do not.

| | IDENTITY | CHANNELS | KNOWLEDGE | DISTRIBUTION |
|---|---|---|---|---|
| HPC (n=44) | 32% | 77% | 44% | 58% |
| QC (n=43) | 31% | 72% | 50% | 56% |

*Mean share of the 9 automated signals present per project*




## 06 WHAT THIS COMMUNITY CAN DO

| | |
|---|---|
| **Maintainer** | **Name your official channels and a fake-reporting path in SECURITY.md. One afternoon.** |
| **Software Stacks** | **Surface channel-provenance signals at install time.** |
| **Facility** | **Request channel provenance in software management plans.** |

***Before you trust a dependency, ask where its community lives.***


**ACKNOWLEDGEMENT:** Conducted under the author's 2025–2026 Trusted CI Fellowship, NSF Cybersecurity Center of Excellence. Portions of the text were drafted with writing assistance from Claude (Anthropic). All content and data were produced and verified by the author.