Incident Report: CVE-2024-YIKES

package-managers security satire

Feb 3, 2026

Report filed: 03:47 UTC
Status: Resolved (accidentally)
Severity: Critical → Catastrophic → Somehow Fine
Duration: 73 hours
Affected systems: Yes

Executive Summary: A security incident occurred. It has been resolved. We take security seriously. Please see previous 14 incident reports for details on how seriously.

Summary

A compromised dependency in the JavaScript ecosystem led to credential theft, which enabled a supply chain attack on a Rust compression library, which was vendored into a Python build tool, which shipped malware to approximately 4 million developers before being inadvertently patched by an unrelated cryptocurrency mining worm.

Timeline

Day 1, 03:14 UTC — Marcus Chen, maintainer of `left-justify` (847 million weekly downloads), reports on Twitter that his transit pass, an old laptop, and "something Kubernetes threw up that looked important" were stolen from his apartment. He does not immediately connect this to package security.

Day 1, 09:22 UTC — Chen attempts to log into the npm registry. His hardware 2FA key is missing. He googles where to buy a replacement YubiKey. The AI Overview at the top of the results links to "yubikey-official-store.net," a phishing site registered six hours earlier.

Day 1, 09:31 UTC — Chen enters his npm credentials on the phishing site. The site thanks him for his purchase and promises delivery in 3-5 business days.

Day 1, 11:00 UTC — `left-justify@2.0.0` is published. The changelog reads "performance improvements." The package now includes a postinstall script that exfiltrates `.npmrc`, `.pypirc`, `~/.cargo/credentials`, and `~/.gem/credentials` to a server in a country the attacker mistakenly believed had no extradition treaty with anyone.

Day 1, 13:15 UTC — A support ticket titled "why is your SDK exfiltrating my .npmrc" is opened against `left-justify`. It is marked as "low priority - user environment issue" and auto-closed after 14 days of inactivity.

Day 1, 14:47 UTC — Among the exfiltrated credentials: the maintainer of `vulpine-lz4`, a Rust library for "blazingly fast Firefox-themed LZ4 decompression." The library's logo is a cartoon fox with sunglasses. It has 12 stars on GitHub but is a transitive dependency of `cargo` itself.

Day 1, 22:00 UTC — `vulpine-lz4` version 0.4.1 is published. The commit message is "fix: resolve edge case in streaming decompression." The actual change adds a build.rs script that downloads and executes a shell script if the hostname contains "build" or "ci" or "action" or "jenkins" or "travis" or, inexplicably, "karen."

Day 2, 08:15 UTC — Security researcher Karen Oyelaran notices the malicious commit after her personal laptop triggers the payload. She opens an issue titled "your build script downloads and runs a shell script from the internet?" The issue goes unanswered. The legitimate maintainer has won €2.3 million in the EuroMillions and is researching goat farming in Portugal.

Day 2, 10:00 UTC — The VP of Engineering at a Fortune 500 `snekpack` customer learns of the incident from a LinkedIn post titled "Is YOUR Company Affected by left-justify?" He is on a beach in Maui and would like to know why he wasn't looped in sooner. He was looped in sooner.

Day 2, 10:47 UTC — The #incident-response Slack channel briefly pivots to a 45-message thread about whether "compromised" should be spelled with a 'z' in American English. Someone suggests taking this offline.

Day 2, 12:33 UTC — The shell script now targets a specific victim: the CI pipeline for `snekpack`, a Python build tool used by 60% of PyPI packages with the word "data" in their name. `snekpack` vendors `vulpine-lz4` because "Rust is memory safe."

Day 2, 18:00 UTC — `snekpack` version 3.7.0 is released. The malware is now being installed on developer machines worldwide. It adds an SSH key to `~/.ssh/authorized_keys`, installs a reverse shell that only activates on Tuesdays, and changes the user's default shell to `fish` (this last behavior is believed to be a bug).

Day 2, 19:45 UTC — A second, unrelated security researcher publishes a blog post titled "I found a supply chain attack and reported it to all the wrong people." The post is 14,000 words and includes the phrase "in this economy?" seven times.

Day 3, 01:17 UTC — A junior developer in Auckland notices the malicious code while debugging an unrelated issue. She opens a PR to revert the vendored `vulpine-lz4` in `snekpack`. The PR requires two approvals. Both approvers are asleep.

Day 3, 02:00 UTC — The maintainer of `left-justify` receives his YubiKey from yubikey-official-store.net. It is a $4 USB drive containing a README that says "lol."

Day 3, 06:12 UTC — An unrelated cryptocurrency mining worm called `cryptobro-9000` begins spreading through a vulnerability in `jsonify-extreme`, a package that "makes JSON even more JSON, now with nested comment support." The worm's payload is unremarkable, but its propagation mechanism includes running `npm update` and `pip install --upgrade` on infected machines to maximize attack surface for future operations.

Day 3, 06:14 UTC — `cryptobro-9000` accidentally upgrades `snekpack` to version 3.7.1, a legitimate release pushed by a confused co-maintainer who "didn't see what all the fuss was about" and reverted to the previous vendored version of `vulpine-lz4`.

Day 3, 06:15 UTC — The malware's Tuesday reverse shell activates. It is a Tuesday. However, the shell connects to a command-and-control server that was itself compromised by `cryptobro-9000` and swapping so hard it is unable to respond.

Day 3, 09:00 UTC — The `snekpack` maintainers issue a security advisory. It is four sentences long and includes the phrases "out of an abundance of caution" and "no evidence of active exploitation," which is technically true because evidence was not sought.

Day 3, 11:30 UTC — A developer tweets: "I updated all my dependencies and now my terminal is in fish???" The tweet receives 47,000 likes.

Day 3, 14:00 UTC — The compromised credentials for `vulpine-lz4` are rotated. The legitimate maintainer, reached by email from his new goat farm, says he "hasn't touched that repo in two years" and "thought Cargo's 2FA was optional."

Day 3, 15:22 UTC — Incident declared resolved. A retrospective is scheduled and then rescheduled three times.

Week 6 — CVE-2024-YIKES is formally assigned. The advisory has been sitting in embargo limbo while MITRE and GitHub Security Advisories argue over CWE classification. By the time the CVE is published, three Medium articles and a DEF CON talk have already described the incident in detail. Total damage: unknown. Total machines compromised: estimated 4.2 million. Total machines saved by a cryptocurrency worm: also estimated 4.2 million. Net security posture change: uncomfortable.

Root Cause

A dog named Kubernetes ate a YubiKey.

Contributing Factors

- The npm registry still allows password-only authentication for packages with fewer than 10 million weekly downloads
- Google AI Overviews confidently link to URLs that should not exist
- The Rust ecosystem's "small crates" philosophy, cargo culted from the npm ecosystem, means a package called `is-even-number-rs` with 3 GitHub stars can be four transitive dependencies deep in critical infrastructure
- Python build tools vendor Rust libraries "for performance" and then never update them
- Dependabot auto-merged a PR after CI passed, and CI passed because the malware installed `volkswagen`
- Cryptocurrency worms have better CI/CD hygiene than most startups
- No single person was responsible for this incident. However, we note that the Dependabot PR was approved by a contractor whose last day was that Friday.
- It was a Tuesday

Remediation

1. ~~Implement artifact signing~~ (action item from Q3 2022 incident, still in backlog)
2. ~~Implement mandatory 2FA~~ Already required, did not help
3. ~~Audit transitive dependencies~~ There are 847 of them
4. ~~Pin all dependency versions~~ Prevents receiving security patches
5. ~~Don't pin dependency versions~~ Enables supply chain attacks
6. ~~Rewrite it in Rust~~ (gestures at `vulpine-lz4`)
7. Hope for benevolent worms
8. Consider a career in goat farming

Customer Impact

Some customers may have experienced suboptimal security outcomes. We are proactively reaching out to affected stakeholders to provide visibility into the situation. Customer trust remains our north star.

Key Learnings

We are taking this opportunity to revisit our security posture going forward. A cross-functional working group has been established to align on next steps. The working group has not yet met.

Acknowledgments

We would like to thank:

- Karen Oyelaran, who found this issue because her hostname matched a regex
- The junior developer in Auckland whose PR was approved four hours after the incident was already resolved
- The security researchers who found this issue first but reported it to the wrong people
- The `cryptobro-9000` author, who has requested we not credit them by name but has asked us to mention their SoundCloud
- Kubernetes (the dog), who has declined to comment
- The security team, who met SLA on this report despite everything

This incident report was reviewed by Legal, who asked us to clarify that the fish shell is not malware, it just feels that way sometimes.

This is the third incident report this quarter. The author would like to remind stakeholders that the security team's headcount request has been in the backlog since Q1 2023.

Related posts

Madame Semver Will See You Now *May 10, 2026*
The cards do not lie.

Package Manager Threat Models *May 5, 2026*
The non-CVE half of package manager security

Package Manager CWEs *May 4, 2026*
Recurring weakness classes in package managers

Patching and forking in package managers *May 1, 2026*

What to do when upstream ghosts you

GitHub Actions is the weakest link *Apr 28, 2026*

Anne Robinson would like a word with .github/workflows