

TuxCare Releases 2026 Open Source Landscape Report

PALO ALTO, CA, UNITED STATES, February 18, 2026 /EINPresswire.com/ -- [TuxCare](#), a global innovator in securing open source, today announced the release of its 2026 Open Source Landscape Report. The third annual report captures how organizations are actually running open-source software (OSS) in production – what broke, what changed, and what works.



Download the complete 2026 Open Source Landscape Report at:
<https://tuxcare.com/2026-open-source-landscape-report/>

Throughout Q4 2025, TuxCare researchers gathered data from a predominantly technical respondent base. Software engineers represented the largest segment of participants, followed by tech leads, system administrators, and DevOps professionals. Security-focused roles were well represented, including application security analysts and IT security analysts. This distribution underscores that the report's findings are shaped primarily by practitioners directly responsible for implementation, uptime, and risk management – rather than by executive, procurement, or policy-only perspectives.

TuxCare's researchers delivered insights across critical areas shaping enterprise OSS strategy, including:

Security Incidents Are a Routine Reality for Many Organizations

Among respondents who were aware of their organization's incident status, 47.8% reported experiencing a cybersecurity incident in the past 12 months. The near-even split indicates that incidents appear to be neither rare nor universal, as reported by enterprise open-source users, but they are frequent enough to be considered a normal operating risk for a large share of organizations.

A Majority of Reported Incidents Remain Associated With Unapplied Patches

Among the open-source users whose organizations reported a cybersecurity incident, 61.4%

indicated that the incident occurred when a patch was available but had not been applied – a slight increase from 60.4% last year. The connection between cybersecurity incidents and unapplied vulnerability patches appears persistent rather than improving or deteriorating significantly. The lack of material change compared with last year suggests that organizations continue to face similar constraints around patch timing, deployment, and prioritization.

Open-Source Lifecycle Tracking Is The New Normal

One of the more revealing findings is that internal tracking or dependency tools don't prevent organizations from being caught off guard by EOL-related breakages and scan findings that flag end-of-life dependencies. While these tools are effective at identifying what exists in the environment, they often fail to reveal lifecycle risk early (such as an approaching EOL) unless paired with clear ownership, review cadence, and accountability. This reinforces a critical distinction: lifecycle awareness is not a tooling problem alone, but an operational effort that tools must be designed to support.

In addition to the most notable findings above, the report covers the following critical areas in detail:

- Open-Source Technologies in Use
- Open-Source Security Incidents
- Linux Patch and Vulnerability Management
- OSS Lifecycle Management
- Open-Source Supply Chain Security

[Click here](#) to download the entire report.

About TuxCare

TuxCare is on a mission to reduce the risk of cyber exploitation while making it easier for enterprises to get the most from their open-source technologies. Through its automated rebootless vulnerability patching solutions, end-of-life security offerings, and enterprise-grade support for AlmaLinux, TuxCare empowers thousands of organizations to protect themselves while leveraging the most advanced enterprise security solutions on the market today. The world's largest enterprises, government agencies, service providers, universities, and research institutions are protected by TuxCare on over one million workloads and growing. For more information, go to <https://tuxcare.com>.

DeShea Witcher

TuxCare

marketing@tuxcare.com

This press release can be viewed online at: <https://www.einpresswire.com/article/893432663>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.