Black Duck Newsroom

Black Duck Research Shows Open Source Vulnerabilities Have Doubled as AI Accelerates Code Creation

2026 OSSRA report highlights the rapidly expanding attack surface and abrupt rise in open source vulnerabilities and license conflicts in commercial codebases

BURLINGTON, Mass., Feb. 25, 2026 /PRNewswire/ -- Black Duck®, the leader in AI-powered application security, today released the 2026 Open Source Security and Risk Analysis (OSSRA) report, revealing the largest increases in open source security, licensing, and operational risk since the report's inception.

Based on analysis of 947 codebases across 17 industries, the findings capture a software ecosystem transformed by AI-assisted development, where code, dependencies, and risks are being introduced at unprecedented speed. The OSSRA's data is powered by the Black Duck KnowledgeBase™, the world's most complete open source intelligence repository.

Open source has become effectively universal, appearing in 98% of codebases, meaning almost every application now inherits third-party risk. Meanwhile, AI-generated code and AI model integration have introduced new forms of risk not previously captured at scale.

Key findings include:

- **An Expanding Attack Surface**. The 2026 OSSRA report shows an unprecedented year of acceleration, with mean vulnerabilities per codebase jumping 107%. Additionally, open source component counts increased 30% year-over year, and the number of files per codebase grew 74%. According to the report, AI model adoption has also created a new, unregulated attack surface.
- **AI is increasing legal and licensing exposure.** AI-generated code creates new IP and license risks as models may reproduce code governed by restrictive licenses (i.e., GPL; AGPL). In fact, the 2026 OSSRA report found that two-thirds of audited codebases contain license conflicts – the highest rate in OSSRA history. A 12% increase identified this year (68% compared to 56% last year) represents the largest single-year jump the study has recorded.
- **Governance has not caught up to AI adoption.** The maturity gap is stark: Black Duck research previously found that 76% of surveyed organizations check AI-generated code for security risks, but only 54% evaluate it for IP and license risks, and just 56% assess quality issues. Altogether, only 24% perform comprehensive IP, license, security, and quality evaluations for AI-generated code. The 2026 OSSRA report warns that organizations cannot comply with upcoming regulations – such as the EU Cyber Resilience Act (CRA) – unless they track AI models with the same rigor as open source components, improve SBOM accuracy and vulnerability workflows, and develop clear AI usage and retraining policies.

"AI has fundamentally changed the economics of software development—and with it, the economics of software risk," said Jason Schmitt, CEO at Black Duck. "This year's OSSRA findings underscore a truth the industry can no longer ignore: the pace at which software is created now exceeds the pace at which most organizations can secure it. Companies that fail to modernize their supply chain governance risk are falling behind not only technologically, but competitively."

Visibility has become the new currency of trust. Whether it's open source components, transitive dependencies, or embedded AI models, organizations must know what's in their software before their customers—and regulators—ask the question.

To learn more, download the 2026 OSSRA report and read the detailed blog post.

About Black Duck

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.

SOURCE Black Duck Software

For further information: Liz Samet, Black Duck, 336.414.6753, esamet@blackduck.com

---

https://news.blackduck.com/2026-02-25-Black-Duck-Research-Shows-Open-Source-Vulnerabilities-Have-Doubled-as-AI-Accelerates-Code-Creation