

Black Duck KnowledgeBase

The Most Comprehensive Database of Open Source Software

Deep vulnerability insight and complete license data for millions of open source components, all baked into your applications and containers

Overview

With millions of open source projects available globally from thousands of websites and forges, it is very difficult for development and DevOps teams to accurately and completely track the open source components used to build their applications and containers. But if you don't track open source, you can't manage the security, compliance, and code quality risks that come with its use.

Broad coverage, verified data

The Black Duck KnowledgeBase™ is the backbone of the open source security and management solutions from Synopsys. It is maintained by the Synopsys Cybersecurity Research Center ([CyRC](#)), the industry's most experienced team of open source experts, who ensure data completeness and accuracy.

The Black Duck KnowledgeBase enables accurate identification of the components that compose your applications by indexing the world's open source projects: more than 4.5 million projects from over 24,000 repositories and forges, including public repositories like GitHub and SourceForge, language-specific repos like RubyGems and PyPI, and individual project sites like MySQL. Black Duck helps you protect intellectual property and avoid license noncompliance by tracking over 2,750 open source licenses. Strengthen your application security posture by automatically mapping your open source bill of materials to our database of vulnerabilities from sources including the National Vulnerability Database (NVD), third-party intelligence resources, and CyRC's independent security research teams.

By combining premier open source security and license data with the industry's most powerful and feature-rich open source risk management solutions, only Synopsys gives development, security, and legal teams more visibility and control over open source in applications and containers from development and into production.

Expansive coverage

- 4.5 million unique open source projects
- Over 24,000 forges and repositories, including these:
 - GitHub, SourceForge, RubyGems, PyPI, Google Code, npm, Maven
 - Distros like Debian, Red Hat, Ubuntu, and CentOS and container distros like Alpine
- More than 90 programming languages:
 - Java, Scala
 - C, C++
 - Objective-C, Swift, Go
 - JavaScript, Node.js
 - C#, VB.NET
 - PHP, Perl, Python, Ruby
- Additionally, Black Duck's proprietary codeprint analysis is language agnostic. This scanning approach searches for signatures based on file and directory layouts along with other metadata that is independent of language.

Comprehensive security

- More than 157,000 vulnerabilities
- National Vulnerability Database (NVD)
 - CVE information
 - Severity ratings
- Black Duck Security Advisories
 - Independently sourced and curated
 - Augmented vulnerability details and remediation guidance
 - Tracks more open source vulnerabilities than NVD alone, with thousands of vulnerabilities not tracked by the NVD
 - Same-day vulnerability notifications, weeks earlier than NVD
 - Exploit information (age, manifestation, available fixes)
 - Workarounds, mitigating factors, and compensating controls
 - Indicators of attack and impact analysis
 - CVSS 2 and 3.x scoring, including temporal metrics
 - Vulnerability impact analysis to determine if the vulnerability is reachable

Complete project data

- Detailed project information
 - Version history
 - Indications of support
 - Community size and activity
 - Code reuse and prevalence
- Complete insight for more than 2,750 licenses
 - Verified full license text
 - Obligations and conflict information
 - Subproject licenses
 - Deep license and copyright data

Pinpoint accuracy

- The Synopsys Cybersecurity Research Center continuously monitors major global repositories and vulnerability databases, aggregating, validating, refining, and updating component metadata for accuracy.
- Black Duck CodePrints™ profile actual project code to ensure that source code, dependencies, and code snippets provide the most complete discovery of open source in use, even if it was modified.
- The Black Duck KnowledgeBase receives hourly vulnerability and project data updates on the latest security, license, and quality risks affecting open source in the codebase.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com