FIND & FIX OPEN SOURCE VULNERABILITIES

The Black Duck Hub helps security and development teams identify and mitigate open source related risks across an application portfolio.

Use the Black Duck Hub to:

- Scan code to identify specific open source in use
- Automatically map known vulnerabilities to open source in use
- Triage – assess risk and prioritize vulnerabilities
- Schedule and track remediation
- Identify licenses and community activity

While other static analysis solutions focus on uncovering code related vulnerabilities introduced by developers as they write code, these techniques only catch a small percentage of vulnerabilities reported over time. Vulnerabilities like Heartbleed, Shellshock, Poodle, and Ghost have highlighted the level of exposure that commonly used open source components can cause. These widely publicized vulnerabilities represent only a small fraction of the more than 4,000 open source vulnerabilities reported each year.

Only Black Duck provides:

- The most comprehensive language coverage and development tools integration
- The industry's most complete open source software KnowledgeBase
- Integrated remediation tracking and management

SECURITY STARTS WITH VISIBILITY

Gaining visibility into what open source is in your codebase is the first step in securing open source.

VULNERABILITY DATA:
38% MORE, 3 WEEKS EARLIER

Black Duck provides Hub users access to premium vulnerability data. VulnDB reports 38 percent more vulnerabilities than the NVD, offers deeper insight, and publishes known vulnerabilities three weeks sooner.

Visibility means knowing not only what open source libraries are in use, but also where and how they are used. The Black Duck Hub continuously scans your code to identify specific open source libraries and versions. Updated regularly from the National Vulnerability Database (NVD) and from VulnDB, a more comprehensive and timely vulnerability database, the Black Duck® KnowledgeBase™ maps the open source libraries with critical metadata on vulnerabilities, licensing, community activity, and versions.

The Black Duck Hub continuously scans your projects for newly introduced open source, and helps you manage security vulnerabilities before they become problems. It enables you to review and prioritize vulnerabilities, assign remediation dates, and track closure. Black Duck Hub automatically monitors for new vulnerabilities that are later reported against open source libraries in use within your applications, enabling you to quickly respond to newly identified vulnerabilities.

MAIN FEATURES OF THE BLACK DUCK HUB

Rapid Scanning & Identification	Know your code. Hub's automated scanning capability identifies and inventories all the open source in your applications and containers, including components not declared in package files.
Build-Tool Integrations	Integrate Hub with your continuous integration (CI) environment using the Jenkins plug-in to further automate scanning, identification, and population of an open source bill of materials.
Customizable Bill of Materials (BOM)	Maintain code visibility with an editable open source BOM, combining results from automated scanning, build-tool and package-manager manifests, and manual entries.
Comprehensive Open Source Database	Utilize the Black Duck KnowledgeBase™, the world's most comprehensive database of more than 1 million open source projects for accurate discovery, reliable identification and real-time vulnerability mapping of the open source in use within your projects.
Automatic Vulnerability Mapping & Alerts	Identify known vulnerabilities associated with the open source in your applications and get alerts when new vulnerabilities affecting you are reported. Access more vulnerabilities and receive earlier notifications with the VulnDB add-on option.
Vulnerability Research Tools	Search vulnerabilities by CVE number, vulnerability ID, or name to access vulnerability information from multiple sources, including the National Vulnerability Database (NVD) and VulnDB. Drill down into the details of any vulnerability to further analyze risk, identify all internal project versions affected, locate source files, and view/track remediation progress.
Remediation Tracking	Track planned and actual vulnerability remediation progress within individual projects. Easily import remediation reports into 3rd party tools via a CSV export feature.
Policy Management	Set policies for open source projects, license types, and vulnerability tolerance. Quickly identify policy violations and manage exceptions by project and component.
Risk Dashboards and Reports	Analyze risks within and across projects with easy-to-understand security, license, community activity risk, and remediation-progress dashboards and reports.
IBM AppScan Enterprise Integration	View and manage application security risks across open source and custom code through a single dashboard when using Black Duck Hub and IBM AppScan together.

ABOUT BLACK DUCK SOFTWARE

Organizations worldwide use Black Duck Software's industry-leading products to secure and manage open source software, eliminating the pain related to security vulnerabilities, compliance, and operational risk. Black Duck is headquartered in Burlington, MA and has offices in Mountain View, CA, London, Frankfurt, Hong Kong, Tokyo, Seoul, and Beijing. For more information visit www.blackducksoftware.com.

CONTACT

To learn more, please contact: sales@blackducksoftware.com or +1 781.891.5100
Additional information is available at: www.blackducksoftware.com

BLACKDUCK