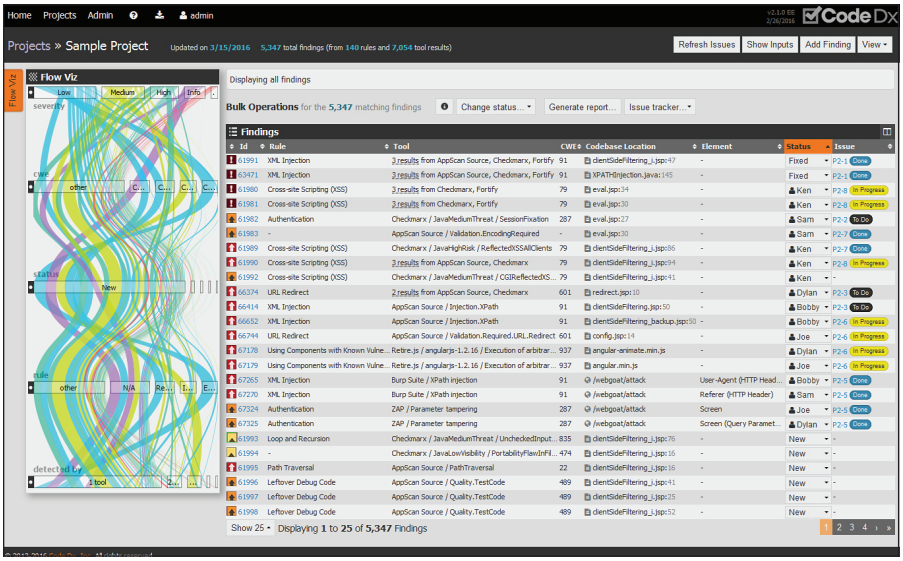
Code Dx

FACT SHEET

Find, prioritize and manage software vulnerabilities, **fast and affordably**



Code Dx is a software vulnerability management system that brings together a variety of code analysis tools that enable you to locate and fix vulnerabilities in the code you write, in the languages you use, and at a low cost.

THE PROBLEM

Over 90% of computer security incidents are due to weaknesses in software. These weaknesses can expose vulnerabilities that put your business at risk for attacks such as SQL injection and cross-site scripting, leading to data loss, corruption, or even a host takeover. Static and dynamic code analysis tools can help you find these weaknesses. However, commercial tools are typically costly, and while open source tools are "free," they still require considerable human resources to configure and run. Regardless of whether you are running a commercial or open source code analysis tool, no single tool provides sufficient code coverage. You have to run multiple tools, and tediously correlate the results.

THE SOLUTION

Code Dx runs a suite of preconfigured, fully integrated, multi-language, open source static code analysis tools against your code base. It can also incorporate the results of commercial static and dynamic tools, and manual analysis, and automatically correlates all the weaknesses into a single consolidated set, viewable from a single user interface—with customizable reports presented in an easy to understand visual display.

KEY BENEFITS

Enhanced Vulnerability Coverage

- Discovery of more weaknesses than any single analysis tool
- Higher confidence in detecting weaknesses with multiple tools

Efficient and Prioritized Remediation

- Rapid triage of false positives
- Improved assessment of severity and criticality
- Source code linked to vulnerabilities
- De-duplication of results

Enhanced Collaboration

- Security and development teams now have a shared tool to communicate findings and discuss remediation

SDLC Tool Support

- Support for integrated development environments (IDEs), continuous integration environments, version control systems, and issue tracking systems

Visualization and Interaction

- More understandable data format
- Focus on the most important weaknesses determined by the user

Easy to Get Started

- Fast and easy installation – up and running in 10 minutes
- Automatically runs bundled open source SAST tools
- Supports multiple DAST tools
- Affordably priced for small-to-medium sized businesses

Who uses Code Dx?

- Software Developers
- Security Analysts
- Software Testers
- Quality Assurance Analysts
- Compliance Auditors
- Accreditors
- CISOs

Uses

- Secure software development
- Security & Quality Assurance reviews
- Verification & Accreditation support
- Compliance reviews
- Code audits
- Pre-procurement software evaluations

Code Dx Standard Edition (SE)

The Standard Edition gives you the power to start writing secure applications quickly, efficiently and inexpensively. Just load your source code into Code Dx and it will automatically select the appropriate tools for finding weaknesses.

Code Dx Enterprise Edition (EE)

The Enterprise Edition provides all of the powerful features of the Standard Edition—and it expands your coverage by working seamlessly with commercial static and dynamic testing tools. At the same time, it allows for findings to be added manually. The correlation, normalization and de-duplication of results from multiple tools produces a consolidated set of results, with greater coverage of vulnerabilities and a better assessment of your overall software security risk.

KEY FEATURES

- Contains over 1,500 configurable security/quality rules covering multiple programming languages
- Automatically configures and runs many bundled static source code analysis tools
- Checks third-party software component libraries for known vulnerabilities
- Maps results to the Common Weakness Enumeration (CWE) and industry standards (OWASP Top 10, SANS Top 25, PCI-DSS and others)
- Combines and normalizes the output of multiple SAST tools, third party vulnerabilities, DAST tools (EE only) and manual findings (EE only) into a single consolidated set of results on a common severity scale.
- Merges duplicate results with customizable correlation logic.
- Visual analytics for triage and prioritization of software weaknesses
- Robust data filtering supports detailed drill-down and organization of weaknesses
- Links correlated weaknesses to specific line of source code
- Search filter capability enables in-depth exploration of results
- Browser-based user interface used to assign, collaborate, and track weakness remediation
- Generates customizable CSV, XML and PDF assessment reports
- Plug-ins provide support for popular Integrated Development Environments (Eclipse/Visual Studio) and continuous integration environments (Jenkins)
- REST API enables integration with automated build servers
- Integrates with the popular JIRA Issue Tracker and provides support for custom JIRA fields
- Integrates with the Git Version Control System
- Supports XML input for integration to custom or proprietary analysis tools

Specifications

Code Dx is a browser-based application that you install locally. The application runs on Windows, Linux and Mac platforms, and all modern browsers are supported.

About Code Dx

Code Dx grew out of research funded by the Department of Homeland Security Science & Technology (DHS S&T) Directorate. DHS is committed to improving the security of the nation's information infrastructure.

Code Dx is proud to be a part of the DHS S&T Software Assurance Marketplace (SWAMP), a collaborative marketplace for continuous software assurance.

FEATURE COMPARISON		(SE)	(EE)
Operating system support			
Windows (7, 8, 10 & Server 2012 R2+)		✔	✔
Mac OS X 10.8+		✔	✔
Linux (Ubuntu, Fedora, Debian, RHEL, and CentOS)		✔	✔
Language support			
C / C++		✔	✔
Java		✔	✔
Javascript		✔	✔
JSP		✔	✔
.NET (C#, Visual Basic)		✔	✔
Python		✔	✔
Ruby		✔	✔
Free & open source SAST tool support			
Android Lint	Clang		✔
ErrorProne	Jlint		✔
OCLint			✔
Brakeman	CAT.NET	✔	✔
CheckStyle	CppCheck	✔	✔
FindBugs	FxCop	✔	✔
Gendarme	JSHint	✔	✔
PMD	Pylint	✔	✔
Commercial SAST tool support			
Checkmarx	Coverity		✔
HP Fortify	IBM AppScan		✔
Parasoft	Veracode		✔
Armorize CodeSecure			✔
GrammaTech Code Sonar			✔
WhiteHat Sentinel Source			✔
Free, open source & commercial DAST tool support			
Acunetix	Arachni		✔
Burp Suite	HP Webinspect		✔
IBM AppScan	Netsparker		✔
OWASP ZAP	Veracode		✔
WhiteHat Sentinel Dynamic			✔
3rd party software library checkers			
OWASP Dependency-Check		✔	✔
Retire.js		✔	✔
IDE support			
MS Visual Studio		✔	✔
Eclipse		✔	✔
Issue tracking support			
JIRA		✔	✔
Continuous integration support			
Jenkins		✔	✔
REST API		✔	✔
Version control system support			
Git		✔	✔

Code Dx