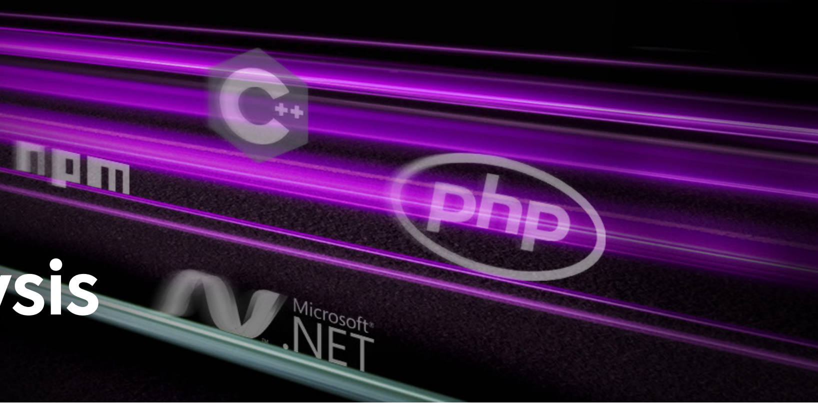
CHECKMARX



Open Source Analysis

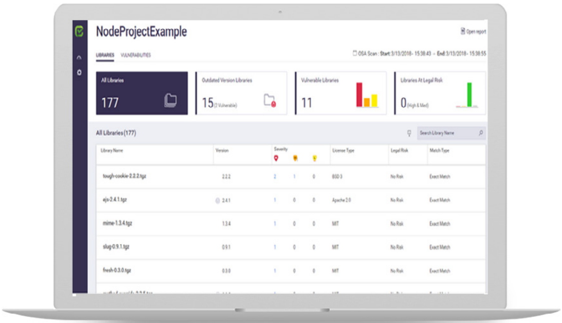
Take Control of your Open Source

Security vulnerabilities and the devastating effect they can have on your organization doesn’t just impact in-house code, they also occur in open source components and libraries. Checkmarx Open Source Analysis (CxOSA) is an open source analysis solution that extends our CxSAST solution to detect, aggregate and manage open source components as part of the CI/CD toolchain.

CxOSA allows organizations to manage, control and prevent the security risks and legal implications introduced by open source components used as part of the software development process. Open source is free, it shortens time-to-market, and has a large development community to test and improve it. However, open source is like any other code - they have security vulnerabilities and bugs that can expose your organization to security risks. Therefore, security measures must be taken to continuously monitor and manage the use of open source components so you can remediate issues early in the development lifecycle.

Unique Solution Benefits

- **Continuously monitor open source code**
  Shift left, remediate earlier, lower costs
- **Integrates seamlessly into the full CxSAST solution**
  Single scanning of both open source and in-house code with easy management to a unified project view
- **Identifies open source vulnerabilities**
  Generate reports with mitigation advice via a unified reports dashboard
- **Easily define and enforce policies for organization compliance**
  Development organizations can set policies to suppress and enforce vulnerability libraries


NodeProjectExample

Open report

LIBRARIES VULNERABILITIES

OSA Scan : Start: 3/13/2018 - 15:38:43 → End: 3/13/2018 - 15:38:55

All Libraries 177

Outdated Version Libraries 15 (2 Vulnerable)

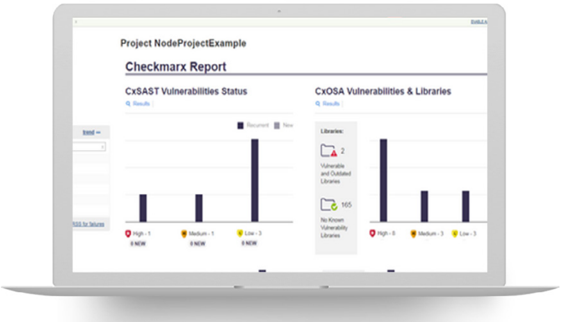
Vulnerable Libraries 11

Libraries At Legal Risk 0 (High & Med)

All Libraries (177)

Search Library Name

Library Name	Version	Severity ●	Severity ●	Severity ●	License Type	Legal Risk	Match Type
tough-cookie-2.2.2.tgz	2.2.2	2	1	0	BSD 3	No Risk	Exact Match
ejs-2.4.1.tgz	2.4.1	1	0	0	Apache 2.0	No Risk	Exact Match
mime-1.3.4.tgz	1.3.4	1	0	0	MIT	No Risk	Exact Match
slug-0.9.1.tgz	0.9.1	1	0	0	MIT	No Risk	Exact Match
fresh-0.3.0.tgz	0.3.0	1	0	0	MIT	No Risk	Exact Match


Project NodeProjectExample

Checkmarx Report

CxSAST Vulnerabilities Status

Results

Recurrent New

High - 1 0 NEW

Medium - 1 0 NEW

Low - 3 0 NEW

CxOSA Vulnerabilities & Libraries

Results

Libraries:

2 Vulnerable and Outdated Libraries

165 No Known Vulnerability Libraries

High - 8

Medium - 3

Low - 3

Initiate and Automate

Initiate testing from a standard web browser or directly inside your build environment (such as Jenkins, Maven, TeamCity, Bamboo, MS-VSTS), and automatically run open source analysis scans with in-house code as part of the CI/CD toolchain. Results are aggregated and reports are generated for display in the web UI or build manager interface in a unified project view.

Manage Security Vulnerabilities

Detect vulnerable and outdated open source libraries to help you prioritize, manage and maintain your application's security posture. Leverage CxOSA to track thousands of common vulnerabilities exposures (CVE), security advisories, and bug trackers so that you will be up to date and receive remediation recommendations that need to be taken to ensure your applications remain secure. Furthermore, developers can also set policies to suppress vulnerability libraries and comply with organization policies.

Legal Compliance

Failure to comply with open source license requirements can also result in legal and business risks. CxOSA helps you ensure that you do not use components in a way that may risk your own intellectual property or impact the progress of your organization.

Vulnerability Management

CxOSA is aligned with CxSAST, allowing developers to manage in-house and open source vulnerabilities in the same manner. As both scans can be initiated together, both in-house and open source vulnerabilities can be managed together.

Policies Management

Set-up automated policies by defining your acceptance, rejection, and internal approval process protocols per open source license type, security vulnerability severity, software bug severity, library age and more. As soon as a developer attempts to add an open source component that is not acceptable according to your policies, you'll get an alert.

Optimize Open Source Selection

Open source selection is easy with the browser plugin. Developers can browse for open source components online and verify if they are appropriate from a security, quality, and license compliance perspective– even before they choose to start using it.

Language Coverage and Accuracy

CxOSA uses well-established vulnerability databases and supports all popular open source programing and scripting languages. The WhiteSource proprietary algorithm minimizes False Positives for faster remediation and reduced costs.

Supported Coding Languages

C++
JS
.NET
node JS
php

About Checkmarx

Checkmarx is the Software Exposure Platform for the enterprise. Over 1,400 organizations around the globe rely on Checkmarx to measure and manage software risk at the speed of DevOps. Checkmarx serves five of the world's top 10 software vendors, four of the top American banks, and many government organizations and Fortune 500 enterprises, including SAP, Samsung, and Salesforce.com. Learn more at Checkmarx.com or follow us on Twitter: @checkmarx.