MEND

The Software Composition Analysis (SCA) Solution

The Challenge

Open source components have become the key building block in today's applications, allowing organizations to build better products, faster. However, open source components introduce their own unique set of security and licence compliance challenges that many organizations may not be equipped for.

The question is: how can organizations harness the power of open source without having to compromise on security, speed, or agility?

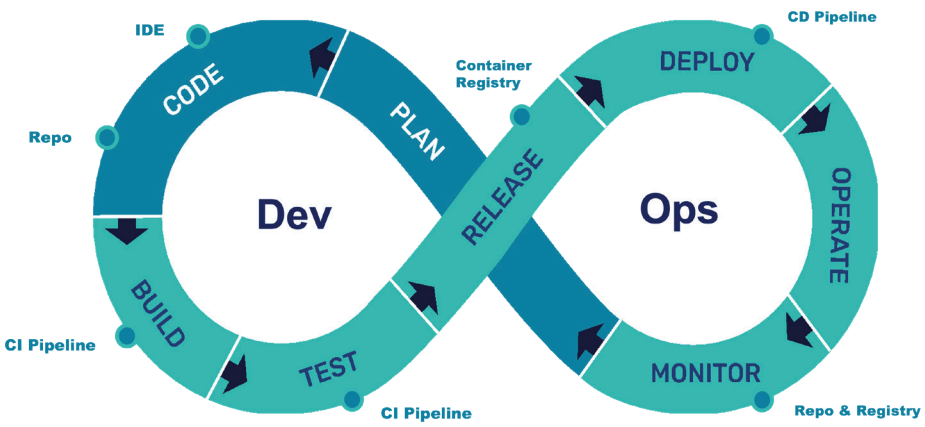
The Mend Solution

Mend allows organizations to gain full visibility and control over their open source usage. It runs silently in the background, detecting all open source components in the code, including all transitive dependencies, every time a build is run or a commit has been performed.

Once detected, the data is cross-referenced with the pre-setup policies to initiate automated workflows, issue alerts in real-time, and offer a wide range of reports available for download.

A Holistic Solution for Open Source Management

Mend supports teams at every step of the software development lifecycle by integrating seamlessly with all environments with one unified agent. Promoting both a shift left and shift right approach to open source security and management, Mend alerts teams on their open source usage from the earliest stages while coding within their native IDE and repository environments, through the build phase, and on to post-deployment.



Key Benefits

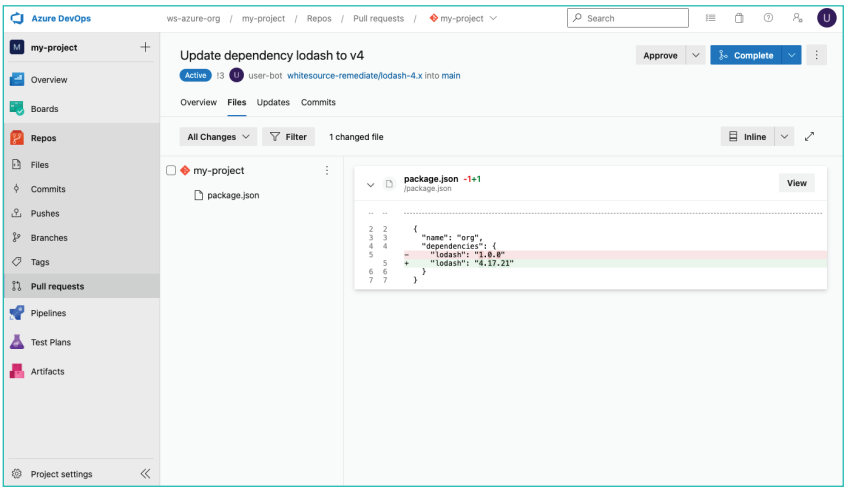
Detection
Identify all open source components, including transitive dependencies, every time you run your build or do a commit.

Prioritization
Focus only on what really matters by guaranteeing no false positives and prioritizing vulnerabilities based on their impact.

Remediation
Speed up remediation with automated fix pull requests, as well as suggested fixes, and automated workflows including Jira and Work item integration.

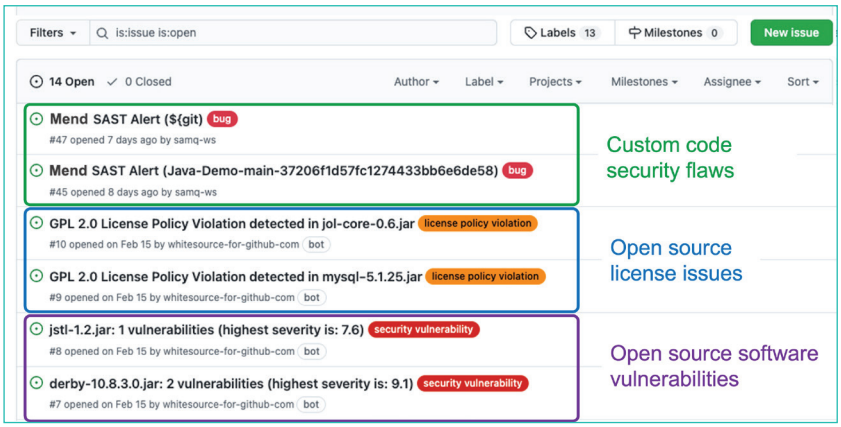
IDE Integration

The IDE integration provides real-time alerts over known open source security vulnerabilities while coding within the IDE UI. When a vulnerable component is detected, icons will appear in the code editor and practical remediation guidance and insights will be suggested.



Repository Integration

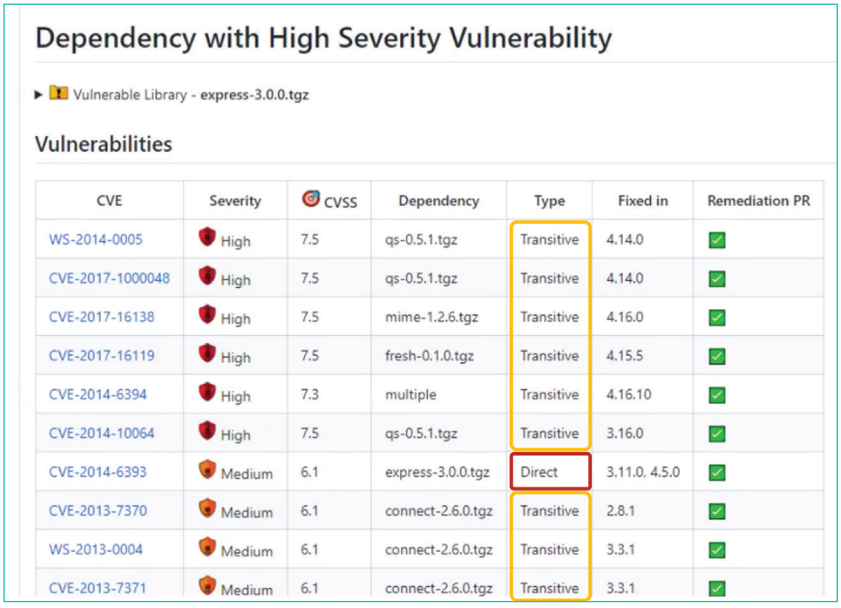
The repository Integration detects all open source components in developers' repos on every commit, alerts on vulnerabilities, and provides suggested fixes, all within the native repo UI. As part of the unified Mend Application Security Platform, Mend SCA shows open source vulnerabilities alongside custom code vulnerabilities and license issues – all within the familiar user interface of the repo.



Direct and Transitive Dependencies

Without Mend, remediation of open source vulnerabilities can be a time-consuming manual process of first knowing how the dependency got into your application, and then figuring out how to fix it.

Mend SCA automatically identifies how the dependency was introduced and automatically creates a pull request with a suggested fix to the base library. This transitive 'awareness' lets you quickly and easily auto-remediate both direct and indirect open source vulnerabilities.



CVE	Severity	CVSS	Dependency	Type	Fixed in	Remediation PR
WS-2014-0005	High	7.5	qs-0.5.1.tgz	Transitive	4.14.0	✓
CVE-2017-1000048	High	7.5	qs-0.5.1.tgz	Transitive	4.14.0	✓
CVE-2017-16138	High	7.5	mime-1.2.6.tgz	Transitive	4.16.0	✓
CVE-2017-16119	High	7.5	fresh-0.1.0.tgz	Transitive	4.15.5	✓
CVE-2014-6394	High	7.3	multiple	Transitive	4.16.10	✓
CVE-2014-10064	High	7.5	qs-0.5.1.tgz	Transitive	3.16.0	✓
CVE-2014-6393	Medium	6.1	express-3.0.0.tgz	Direct	3.11.0, 4.5.0	✓
CVE-2013-7370	Medium	6.1	connect-2.6.0.tgz	Transitive	2.8.1	✓
WS-2013-0004	Medium	6.1	connect-2.6.0.tgz	Transitive	3.3.1	✓
CVE-2013-7371	Medium	6.1	connect-2.6.0.tgz	Transitive	3.3.1	✓