MEND

Vulnerability Database

Securing your open source software depends on the industry's best data

The Most Comprehensive Data in the Industry

When choosing a Software Composition Analysis (SCA) solution, the data behind that solution is the difference between fixing critical open source vulnerabilities and leaving your organization exposed. To reduce risk, enterprises need a solution that continuously monitors your code and also provides actionable remediation advice.

Comprehensive and accurate data is essential:

- Only 15-30% of open source vulnerabilities are reachable. Mend is the only solution that detects and filters out unreachable false positives
- About 20% of all publicly disclosed vulnerabilities are not listed in the National Vulnerability Database (NVD).
- The open source community is highly decentralized, which makes finding and validating vulnerabilities a challenge.

Without accurate data, enterprises can't identify all open source vulnerabilities.

Complete Data Coverage

Mend delivers the most complete vulnerability data available, with detailed technical specs, remediation advice, and deep insights. The Mend Knowledge Team uses machine learning algorithms to look beyond the NVD, exhaustively searching through a myriad of open source ecosystems, combining the power of automation with their industry expertise to validate each vulnerability with pinpoint accuracy.

Because of our unique, proprietary research, Mend delivers the industry's best analysis on tens of billions of open source files, hundreds of millions of open source libraries, and more package managers, technologies, and languages than any other solution available today. Mend is also a CVE Numbering Authority (CNA). We publish new vulnerabilities discovered through our internal processes to the NVD and guide external project maintainers through the process of officially disclosing vulnerabilities.

Based on the strength of our data, our customers feel secure knowing that Mend automatically detects the most vulnerabilities of any solution on the market, while empowering them to make knowledgeable prioritization and remediation decisions.

Key Benefits

Provides the most accurate and comprehensive vulnerability database on the market that leverages machine learning and human analysis

Eliminates 70-85% of alerts by filtering out false positives, reducing noise and saving you time and resources

Delivers actionable remediation advice with crowd-sourced data so you have confidence that fixes won't break the build

Offers the broadest support of languages and technologies of any solution on the market

Detailed vulnerability data curated
and enhanced by our expert Knowledge Team

The Mend Knowledge Team

The Mend Knowledge Team curates and enriches all data to ensure data integrity and deliver deep technical insights with a high level of granularity:

- In addition to the NVD, Mend indexes numerous other sources, such as open source issue trackers and proprietary security advisories, to accurately identify open source vulnerabilities.
- Mend scans GitHub commits/issues to detect potential security vulnerabilities. The Mend Knowledge Team analyzes these to confirm that a vulnerability exists then shares these new vulnerabilities with Mend customers.
- Vulnerabilities are identified at the source code level and not at the package level. Often a vulnerability's CPE location is not specific or contains errors, so the Mend Knowledge Team researches individual articles to better understand where the vulnerability is and whether it impacts your code, effectively eliminating false positives.
- When the Knowledge Team pinpoints a vulnerable method, Mend automatically scans related packages to identify all instances of that vulnerability.
- Mend finds loose files not associated with a package manager by using SHA1 detection to determine whether they have open source origins and what the relevant open source license is.
- The Mend Vulnerability Database offers the fastest updates on the market, with new vulnerabilities reported within one hour of being published.

Key Capabilities

Eliminate False Positives

Many SCA vendors can alert when a call trace exists from the proprietary code to the vulnerable open source method. However, Mend has the unique ability to detect whether no call trace exists in addition to when it does. This enables Mend users to effectively eliminate 70-85% of reported vulnerabilities as false positives to focus on remediating threats that actually impact applications.

Actionable Remediation Advice

Mend's uses extensive crowd-sourced data to identify which libraries are safe to update without fear of breaking the build. Mend gathers this data on GitHub through its open source project Renovate to determine how likely a specific package upgrade is to be backward compatible. Given its popularity, Mend Renovate has access to massive amounts of data, so its recommendations have the highest degree of accuracy on the market.

Vulnerability-Component Association

For each vulnerability in the Mend database, the Mend Knowledge Team identifies the vulnerable source code and verifies that the component is indeed vulnerable. Once confirmed, the vulnerability is attributed to every open source component containing the vulnerable source code. This means Mend has identified far more vulnerable components than are listed in the NVD.

Covering the broadest range of languages and technologies on the market

Mend Vulnerability Database

Languages and technologies supported	200+
Package managers supported	30+
Security advisories supported	30+
Number of packages (versions)	~160M
Number of source libraries (tags)	~60M
Number of source files	~450M
Number of vulnerabilities	~250K
Number of vulnerable libraries	~45M
Time to import new packages / tags	<1Day
Time to import tags from consumed repos	<6 Hours

About Mend

Mend helps organizations accelerate the development of secure software at scale. We provide automated tools that bridge the security knowledge gap, integrating easily into the software development life cycle and going beyond detection with a remediation-first approach. Mend is built on the most comprehensive vulnerability database in the industry, providing the widest coverage for threats and attack vectors. Our solution helps enterprises reduce risk and increase the productivity of their security and development teams. For more information, visit www.Mend.io

Related Resources

Learn more at www.mend.io