mend.io

MEND.IO OPEN-SOURCE RISK REPORT

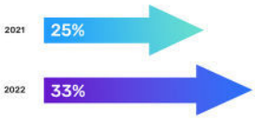
Securing the Software Supply Chain

Open Season on Open-Source Code

Applications are the lifeblood of the global economy, and threat actors know it. As the importance of software supply chains increases, so have the number of attacks launched against them.

More Vulnerabilities, Greater Sophistication, Less Clarity

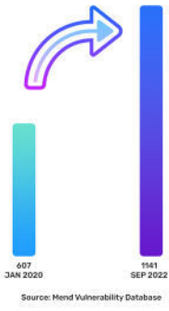
OSS Vulnerabilities On The Rise



- Growth of increasingly sophisticated attacks that incorporate multiple exploits.
- As the number of available vulnerabilities grows, so does the chance of a successful multivector attack.

Permanent Growth Mode

The combination of increased open-source code creation and threat actors motivated to find new holes essentially guarantees that open-source vulnerabilities won't decline any time soon.



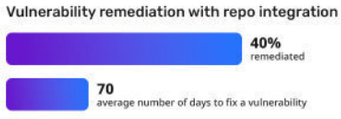
Source: Mend Vulnerability Database

Battling The Remediation Gap

While companies remediated thousands of vulnerabilities each month, many are left with a backlog of untouched vulnerabilities.

We surveyed over 900 companies from January-September 2022:

Next, we took a representative sampling of companies that implemeneted Mend best practices through the repo integration.



The results were telling. The increase in remediated vulnerabilities translates roughly into a **3x reduction in risk**, while the **time to remediation was cut by 75%.**

Malicious Packages: A Growing Challenge

Data from Mend Supply Chain Defender shows a steady quarterly increase in the number of malicious packages published in 2022.

79%
increase from Q2 to Q3 2022

Attacks Grow More Sophisticated

- More packages contain telemetry.
- Malicious code is now built more deeply within the software supply chain.
- Attackers use legitimate hosting providers to ship malicious code.
- Bad actors hide behind domain names, suggesting legitimate use cases.

Prepare For Continued Attack Innovation

3 **average versions per package**

This reflects a learning curve as malicious actors tinker and adjust code between versions.

Mend Predicts

- More advanced evasion techniques.
- Adoption of persistence techniques.
- More diverse and advanced deployment and execution approaches.

Fighting Back

Enterprises need to move beyond today's status quo for application security. Prioritization and remediation tools that target the vulnerabilities that pose the biggest business risk is vital to managing security debt wisely.

Click And Learn More About Open Source Vulnerabilities

mend.io