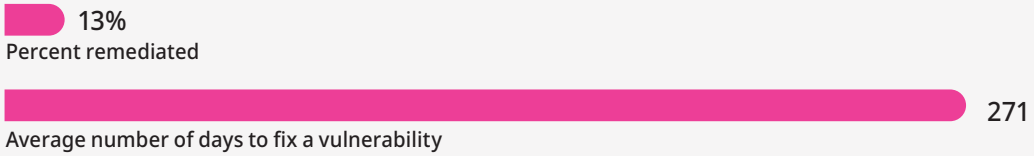
Open Source Security: The View From The User Side

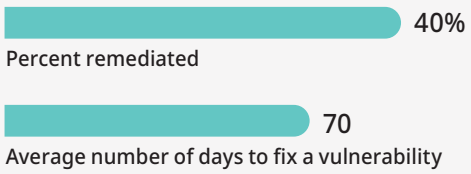
Mend wanted to take a look at open source security from the user perspective. By taking a representative sampling of approximately 1,000 North American companies across industries and company size from January through September 2022, we compiled data on critical and high severity vulnerabilities and remediation to present a snapshot into the state of open source security — and the difference Mend can make.

Baseline vulnerability remediation January-September 2022



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

Vulnerability remediation with repo integration January-September 2022



The results were telling. The increase in remediated vulnerabilities translates roughly into a three times reduction of risk, while the time to remediation was cut by 75 percent.

Remediation gap

While companies remediated thousands of vulnerabilities each month, many are left with a backlog of un-remediated vulnerabilities. Why is this happening? There are a number of reasons why companies face a remediation gap:

Lack of time and resources. It's no secret that application security teams are often overworked and understaffed, leading companies to make hard decisions on what applications to patch and keep current. Some focus on their flagship applications, for example, judging the business risk of not doing so as too high.

Lack of granular information. While the CVE severity index is a reasonable initial metric to use when deciding what to remediate first, it is insufficient for use by itself. It's crucial for application security teams to identify and prioritize vulnerabilities according to the risk they pose, both by themselves and when used in attacks that exploit multiple vulnerabilities. Many vulnerabilities, for example, do not pose a risk within an application and can be safely ignored if they can be identified. This also means that low and medium severity flaws cannot be neglected, as they can be used in multi-vulnerability attacks.

The need to balance security risk and functional risk. While application security is of foundational importance for business applications, so is the need to keep them functional. This can present knotty problems when deciding whether to patch or upgrade the many open source components and associated dependencies used to build an application. What is the risk that a regression error in a dependency update could cause production problems? Most teams cannot put in the massive amount of work needed to manually review each update. Instead, teams are starting to turn to tools that can automate dependency updates without compromising the functionality of an application.

Excerpted from the Mend Open Source Risk Report