

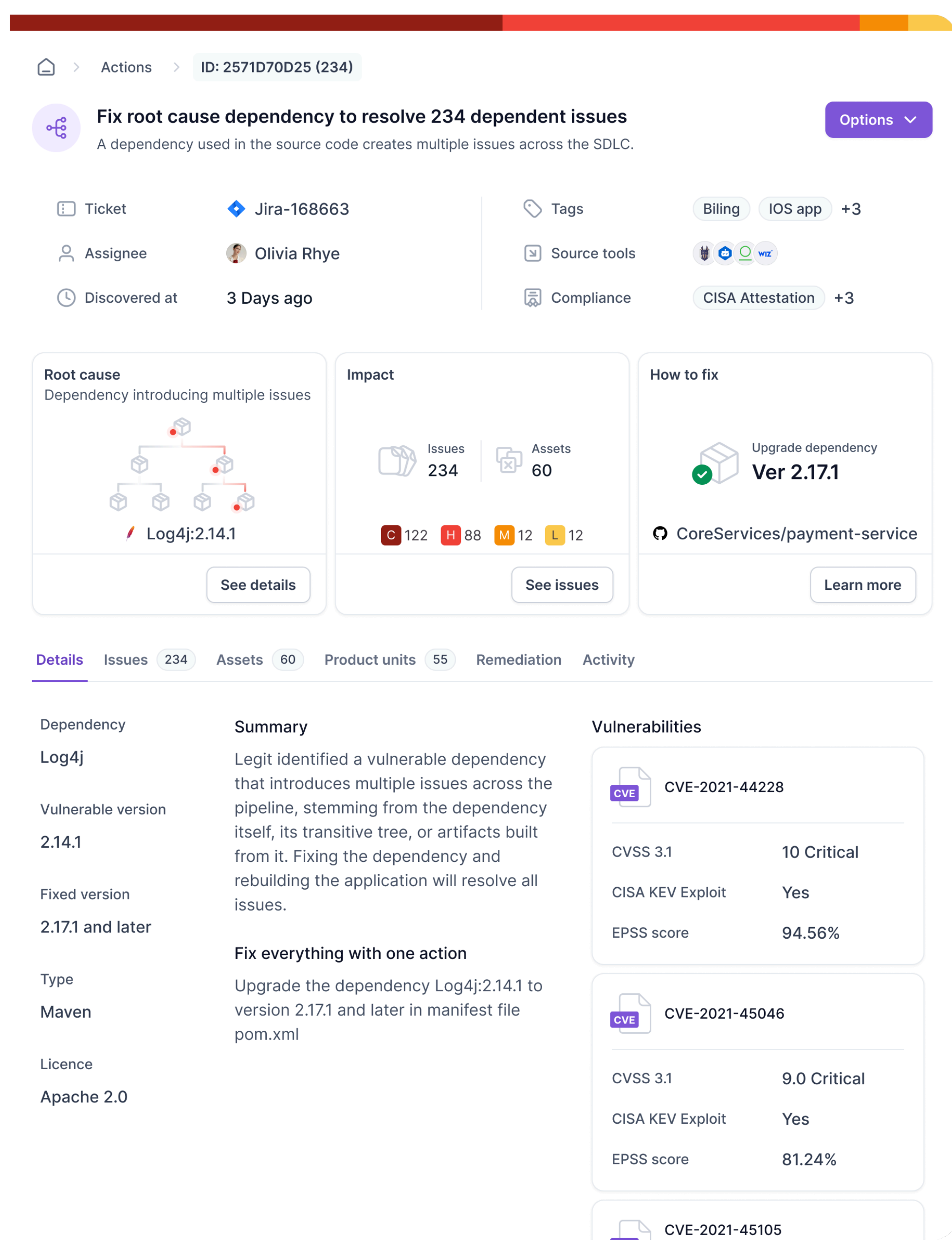
Legit Root Cause Remediation

Fix what matters most with fast, contextual, prioritized, and policy-driven vulnerability remediation

Finding application security issues isn't the problem.

Enterprise security teams face a daily flood of application security findings. Often, many of these vulnerabilities stem from a singular weakness or misconfiguration point, yet they're still typically triaged and remediated individually.

This makes remediating vulnerabilities at scale hard, even with all the necessary context to prioritize vulnerabilities. To effectively reduce the most risk possible, security professionals have to not only understand where an issue originates, but also what issues have the same origination and remediation point, and how to apply a targeted fix at scale.



The screenshot displays a detailed view of a root cause dependency issue. At the top, it shows the issue ID: 2571D70D25 (234). The main heading is "Fix root cause dependency to resolve 234 dependent issues", with a sub-description: "A dependency used in the source code creates multiple issues across the SDLC." There are several metadata fields: Ticket (Jira-168663), Assignee (Olivia Rhye), Discovered at (3 Days ago), Tags (Billing, IOS app +3), Source tools (GitHub, GitLab, Bitbucket, WIZ), and Compliance (CISA Attestation +3). Below this, three key sections are visible: "Root cause" showing a dependency tree for Log4j:2.14.1; "Impact" showing 234 issues and 60 assets, with a breakdown of severity levels (C: 122, H: 88, M: 12, L: 12); and "How to fix" recommending an upgrade to version 2.17.1 for the CoreServices/payment-service. A navigation bar below these sections shows "Details", "Issues 234", "Assets 60", "Product units 55", "Remediation", and "Activity". The main content area is divided into three columns: "Dependency" (Log4j, vulnerable version 2.14.1, fixed version 2.17.1 and later, type Maven, licence Apache 2.0), "Summary" (Legit identified a vulnerable dependency that introduces multiple issues across the pipeline... Fix everything with one action: Upgrade the dependency Log4j:2.14.1 to version 2.17.1 and later in manifest file pom.xml), and "Vulnerabilities" (listing CVE-2021-44228, CVE-2021-45046, and CVE-2021-45105 with their respective CVSS 3.1 scores, CISA KEV status, and EPSS scores).

Legit root cause remediation

The Legit ASPM platform is now the only solution on the market that supports root cause remediation – allowing companies to address multiple issues simultaneously by getting to the true source of the problem.

Focusing on remediation at the root cause of an issue, rather than tackling every vulnerability in isolation, helps AppSec and development speed and scale remediation by getting a one-to-many advantage from fixes applied. Instead of being overwhelmed by endless vulnerabilities, practitioners can prioritize fixes based

on overall impact, reducing risk across the entire organization far more efficiently.

Drawing on deep code and pipeline contextual analysis, Legit pinpoints high-impact fixes that deliver a “one-to-many” remediation. This allows Legit to automatically and easily identify the most bang-for-the-buck fixes, and reduce the time and effort associated with vulnerability remediation, while strengthening customers’ application security postures at scale.

Solve more with less, prioritize for impact, and streamline workflows

Legit root cause remediation helps teams:

Solve more with less: By addressing root causes, one fix can remediate dozens – or even hundreds – of vulnerabilities across repositories, containers, and runtime environments (e.g., updating one package to remedy 60 critical issues across code, containers, and runtime).

Prioritize for impact: Our advanced contextual analysis highlights the most critical remediation tasks first, ensuring your teams focus on what matters most for risk reduction.

Streamline developer workflows: Developers no longer need to apply redundant fixes or hunt down scattered vulnerabilities. Root cause remediation ensures fixes are effective, targeted, and permanent.

Cut friction between security and development: When one ticket solves all findings related to a fix, ticket sprawl dwindles and communication issues subside.

Scaling AppSec while reducing risk

Legit root cause remediation is more than just a feature – it’s a shift in how we approach vulnerability management. By addressing the true source of security issues, teams can scale their AppSec programs, reduce complexity, and improve efficiency without compromising on risk reduction.

Ready to experience the future of application security? With root cause remediation, it’s not just about fixing faster – it’s about fixing smarter.

[Learn More About Legit Security](#)

[Visit our website and Book a Demo](#)

About Legit Security

The Legit Security ASPM platform is a new way to manage application security in a world of AI-first development, providing a cleaner way to manage and scale AppSec and address risks. Fast to implement, easy to use, and AI-native, Legit has an unmatched ability to discover and visualize the entire software factory attack surface, including a prioritized view of AppSec data from siloed scanning tools. As a result, organizations have the visibility, context, and automation they need to quickly find, fix, and prevent the application risk that matters most. Spend less time chasing low-risk findings, more time innovating.