SOLUTION BRIEF

GitLab-Rezilion Integration

THE CHALLENGE
The frequency of new product releases grows daily, creating a challenge for both developers and security teams. DevOps wants to create products and ship them quickly, Security wants to ensure those products are safe. As companies seek to discover vulnerabilities earlier in the development process to meet these demands, new tools are critical to ensure that the velocity of product delivery is not stalled by product security.

The answer? These teams need an integrated solution to validate and prioritize vulnerabilities early on in the development process so that developers can reduce their vulnerability backlog significantly and remediate what matters most without causing delays. The modern development workhorse needs CI tools integrated into their workflow to address this challenge.

Know what is exploitable as you develop—and fix what matters most

GitLab CI is one of the world’s leading CI tools. By integrating directly with GitLab CI, Rezilion’s enhanced run time validation helps customers eliminate what isn’t relevant, so they can focus on what matters most by filtering out anything that does not pose a risk and remediate strategically. With visibility into which software components are loaded to memory and therefore exploitable, customers can reduce the vulnerability backlog significantly. Through the integration, customers will reap the following benefits:

- **Reduce vulnerability backlog by up to 85% and reduce patching efforts** by eliminating un-exploitable vulnerabilities.
- **Prioritize** what matters most in your environment to help save developers time and deliver better products faster.
- **Auto-remediate in hours and not days.** Using validation data from Rezilion’s Next Generation vulnerability database, the Rezilion platform will automatically suggest the best fix available with a new merge request. Saves developers time and addresses risk in a timely manner.
- **Actionable insights within the GitLab CI pipeline.** Non-exploitable vulnerabilities are marked as “false positives” and can be dismissed, while issues can be easily assigned to fix the exploitable ones.
- **Identify software components with a dynamic Software Bill of Materials (SBOM),** including open source components and their loaded/unloaded status for a quick risk view.
- **Shift security** left without shifting work to developers. VEX (Vulnerability Exploitability Exchange) export, providing a standardized format to communicate vulnerabilities and their impact with customers and regulators.
Figure 1: The vulnerability report shows a list of vulnerabilities in the customer’s pipeline and marks them false positives. Additionally, each row shows when it was detected, its status, severity, and details.
Figure 2: The Validated Vulnerabilities report shows all components found in your environment categorized by either loaded/exploitable or unloaded/unexploitable state.

Figure 3: The vulnerable components report shows a list of components found by the vulnerability scanner. Each row represents a component with exploitability context.
**Why is This Integration Important?**

This integration provides GitLab’s customers an immediate view into which vulnerabilities are exploitable and which are not, helping to reduce their vulnerability backlog by up to 70%.

**WHY THIS INTEGRATION MATTERS TO THE CISO, PRODUCT SECURITY, AND DEVELOPERS:**

1. **The CISO is responsible for overall security risk across the platform**
   
   The Rezilion–GitLab integration will help to release products quickly and securely without sacrificing productivity and make SLAs more achievable.

2. **The product security team aims to drive risk reduction.**
   
   The Rezilion–GitLab integration ensures that vulnerabilities are not missed and remediated early on in the process in near real time with minimal effort to ensure the product is delivered on time.

3. **Developers are responsible for delivering products quickly.**
   
   Not knowing what vulnerabilities to fix first results in developers spending time on vulnerabilities that pose no actual risk. The Rezilion–GitLab integration ensures that vulnerabilities are detected, validated, and result in reduction of exploitable vulnerabilities by up to 85% so that developers can auto-remediate quickly and focus on what matters most while addressing 100% of the exploitable risk.
ABOUT REZILION

Rezilion’s platform automatically secures the software you deliver to customers. Rezilion’s continuous runtime analysis detects vulnerable software components on any layer of the software stack and determines their exploitability, filtering out up to 95% of identified vulnerabilities. Rezilion then automatically mitigates exploitable vulnerabilities across the SDLC, reducing vulnerability backlogs and remediation timelines from months to hours, while giving DevOps teams time back to build.

Learn more about Rezilion’s software attack surface management platform at www.rezilion.com and get your 30 day free trial www.rezilion.com.

© Rezilion 2022

Please contact us for your free 30 day trial here.