SOLUTION OVERVIEW

CircleCI-Rezilion Integration Solution Overview

The Challenge

WITH AN UNPRECEDENTED AMOUNT OF PRODUCT RELEASES, developers and security teams are both faced with the challenge of balancing security with delivery. While developers want to develop and ship products quickly, security teams want to ensure that these products are secure. This challenge clearly underlies the need for new tools that will allow organizations to discover and remediate vulnerabilities early in the development process to keep up with the pace of product delivery without compromising product security.

The solution is a cybersecurity tool that integrates seamlessly with your development workflow and allows you to validate and prioritize vulnerabilities early in the development process. This will help developers reduce their vulnerability backlog and remediate vulnerabilities that actually pose a risk without causing delays in product releases.

Know Your Real Attack Surface And Fix What Is Exploitable

CircleCI is one of the world's most popular CI/CD tools. By integrating directly with CircleCI, Rezilion's platform first helps customers discover all software components in their environment. Then using granular run-time validation helps them prioritize vulnerabilities that are exploitable and eliminate what isn't relevant, so they can focus on what matters most and remediate strategically. Following are the key benefits of this integration:

✓ **Reduce vulnerability backlog by 85%** by eliminating un-exploitable vulnerabilities that are not loaded to memory.

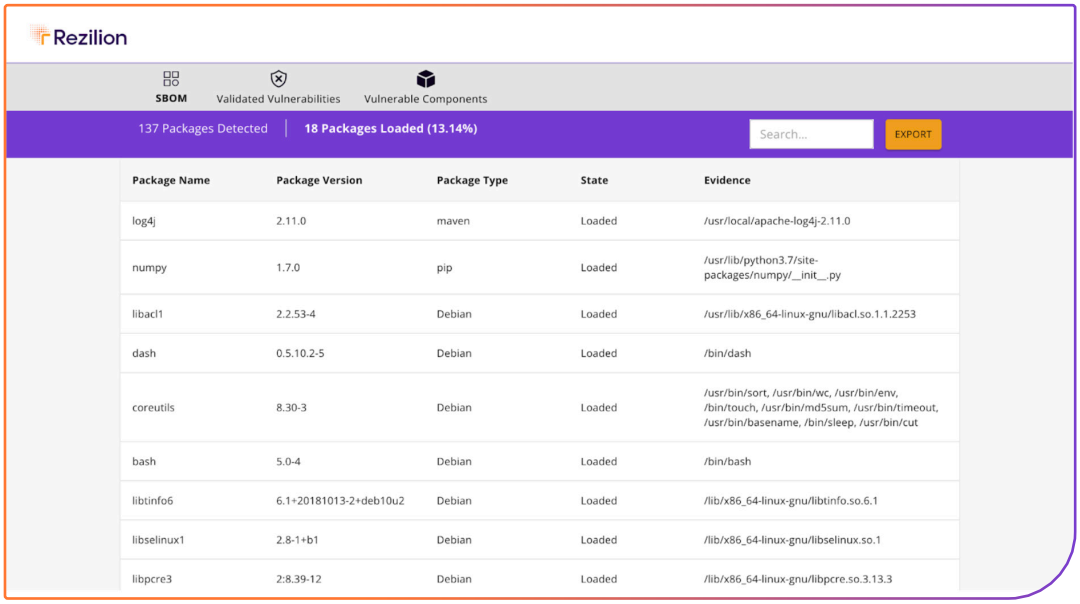
✓ **Reduce patching efforts by** prioritizing what matters most in your environment, thus saving developers many hours and delivering better products faster.

✓ **Reduce remediation timelines from months to hours** with seamless integration into the development workflow that allows timely attention to threats.

✓ **A Dynamic Software Bill of Materials (SBOM)** that quickly provides a comprehensive view of all the software components including open source components including their loaded/unloaded status and exportable in CycloneDX format.

✓ **Shifting left —** Customers can validate vulnerabilities early on the development process — right after the build — as part of the existing testing phase within the CI pipeline.

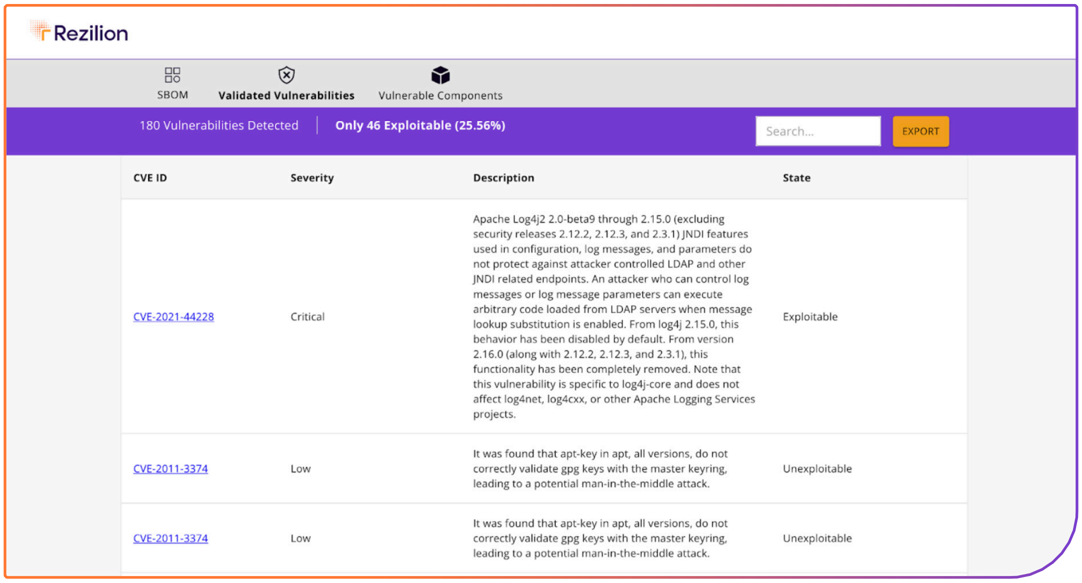
✓ **Actionable insights and easy-to-interpret results —** Customers can view and share reports from within the CircleCI UI that provide actionable insights for taking remediation steps.



137 Packages Detected | **18 Packages Loaded (13.14%)**

Package Name	Package Version	Package Type	State	Evidence
log4j	2.11.0	maven	Loaded	/usr/local/apache-log4j-2.11.0
numpy	1.7.0	pip	Loaded	/usr/lib/python3.7/site-packages/numpy/__init__.py
libacl1	2.2.53-4	Debian	Loaded	/usr/lib/x86_64-linux-gnu/libacl.so.1.1.2253
dash	0.5.10.2-5	Debian	Loaded	/bin/dash
coreutils	8.30-3	Debian	Loaded	/usr/bin/sort, /usr/bin/wc, /usr/bin/env, /bin/touch, /usr/bin/md5sum, /usr/bin/timeout, /usr/bin/basename, /bin/sleep, /usr/bin/cut
bash	5.0-4	Debian	Loaded	/bin/bash
libtinfo6	6.1+20181013-2+deb10u2	Debian	Loaded	/lib/x86_64-linux-gnu/libtinfo.so.6.1
libselinux1	2.8-1+b1	Debian	Loaded	/lib/x86_64-linux-gnu/libselinux.so.1
libpcre3	2:8.39-12	Debian	Loaded	/lib/x86_64-linux-gnu/libpcre.so.3.13.3

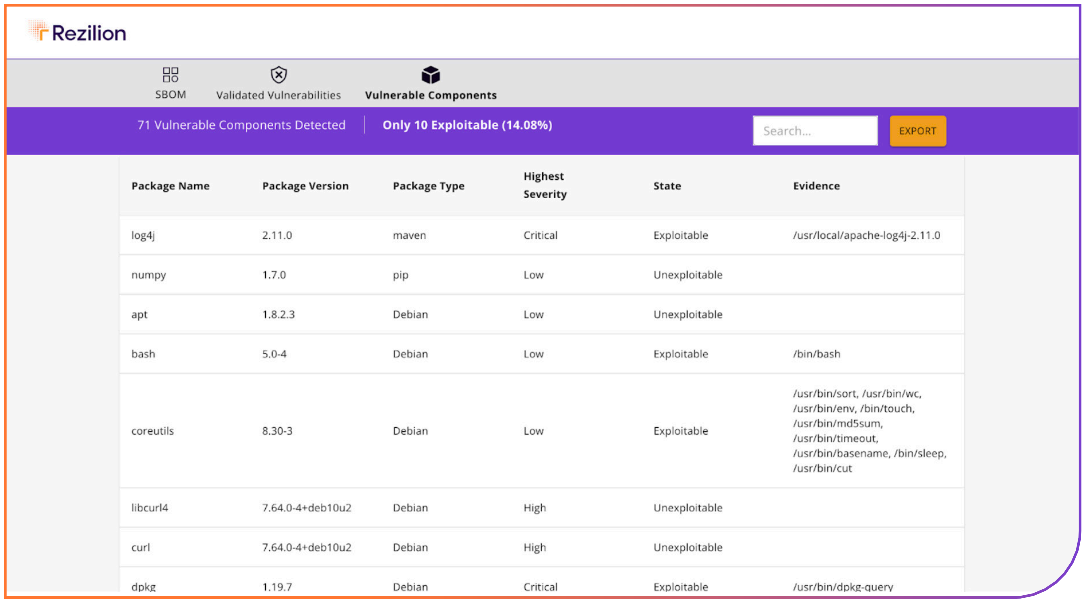
Figure 1: The Dynamic SBOM shows all software components present in your environment.



180 Vulnerabilities Detected | **Only 46 Exploitable (25.56%)**

CVE ID	Severity	Description	State
CVE-2021-44228	Critical	Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.	Exploitable
CVE-2011-3374	Low	It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle attack.	Unexploitable
CVE-2011-3374	Low	It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle attack.	Unexploitable

Figure 2: The validated vulnerabilities report shows all components found in your environment categorized by either loaded/exploitable or unloaded/unexploitable state.



71 Vulnerable Components Detected | **Only 10 Exploitable (14.08%)**

Package Name	Package Version	Package Type	Highest Severity	State	Evidence
log4j	2.11.0	maven	Critical	Exploitable	/usr/local/apache-log4j-2.11.0
numpy	1.7.0	pip	Low	Unexploitable	
apt	1.8.2.3	Debian	Low	Unexploitable	
bash	5.0-4	Debian	Low	Exploitable	/bin/bash
coreutils	8.30-3	Debian	Low	Exploitable	/usr/bin/sort, /usr/bin/wc, /usr/bin/env, /bin/touch, /usr/bin/md5sum, /usr/bin/timeout, /usr/bin/basename, /bin/sleep, /usr/bin/cut
libcurl4	7.64.0-4+deb10u2	Debian	High	Unexploitable	
curl	7.64.0-4+deb10u2	Debian	High	Unexploitable	
dpkg	1.19.7	Debian	Critical	Exploitable	/usr/bin/dpkg-query

Figure 3: The vulnerable components report shows a list of components found by the vulnerability scanner. Each row represents a component with an exploitability context.

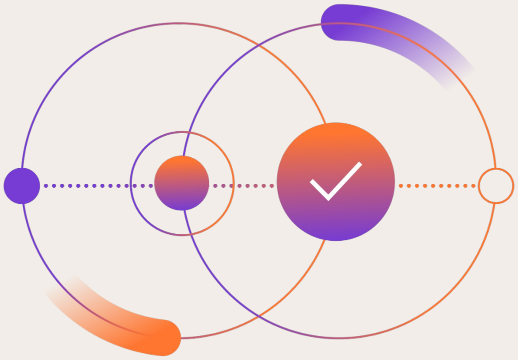
“Why is this Integration Important?”

With this integration, CircleCI users can REDUCE THEIR VULNERABILITY BACKLOG BY 85% and get a quick view into their actual software attack surface.

Why This Integration Matters to the CISO, Product Security, and Developers

1. Developers are focused on delivering products quickly.

Developers are faced with a growing backlog of vulnerabilities and not knowing which vulnerabilities actually matter, they end up spending time on vulnerabilities that pose no actual risk. The Rezilion-CircleCI integration ensures this does not happen by discovering all the vulnerabilities, validating their exploitability, and prioritizing which vulnerabilities to fix first. This reduces the backlog by up to 85% and allows developers to release products quickly by focusing on what matters most.



2. The product security team aims to drive risk reduction.

The Rezilion-CircleCI integration allows product security teams to detect all vulnerabilities early in the development process and remediate them automatically with very little effort for on-time product delivery.

3. The CISO is responsible for overall security risk across the platform.

The Rezilion-CircleCI integration makes sure that vulnerabilities are detected, prioritized and remediation. All the while, products are release quickly and securely without sacrificing productivity and make SLAs more achievable.

Get Started with Rezilion Solutions Learn more about Rezilion's software attack surface management platform at www.rezilion.com and get your 30-day free trial. Or see our platform in action and book a demo at https://www.rezilion.com/request-a-demo/.

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.