Rezilion | GitLab

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 proces 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.

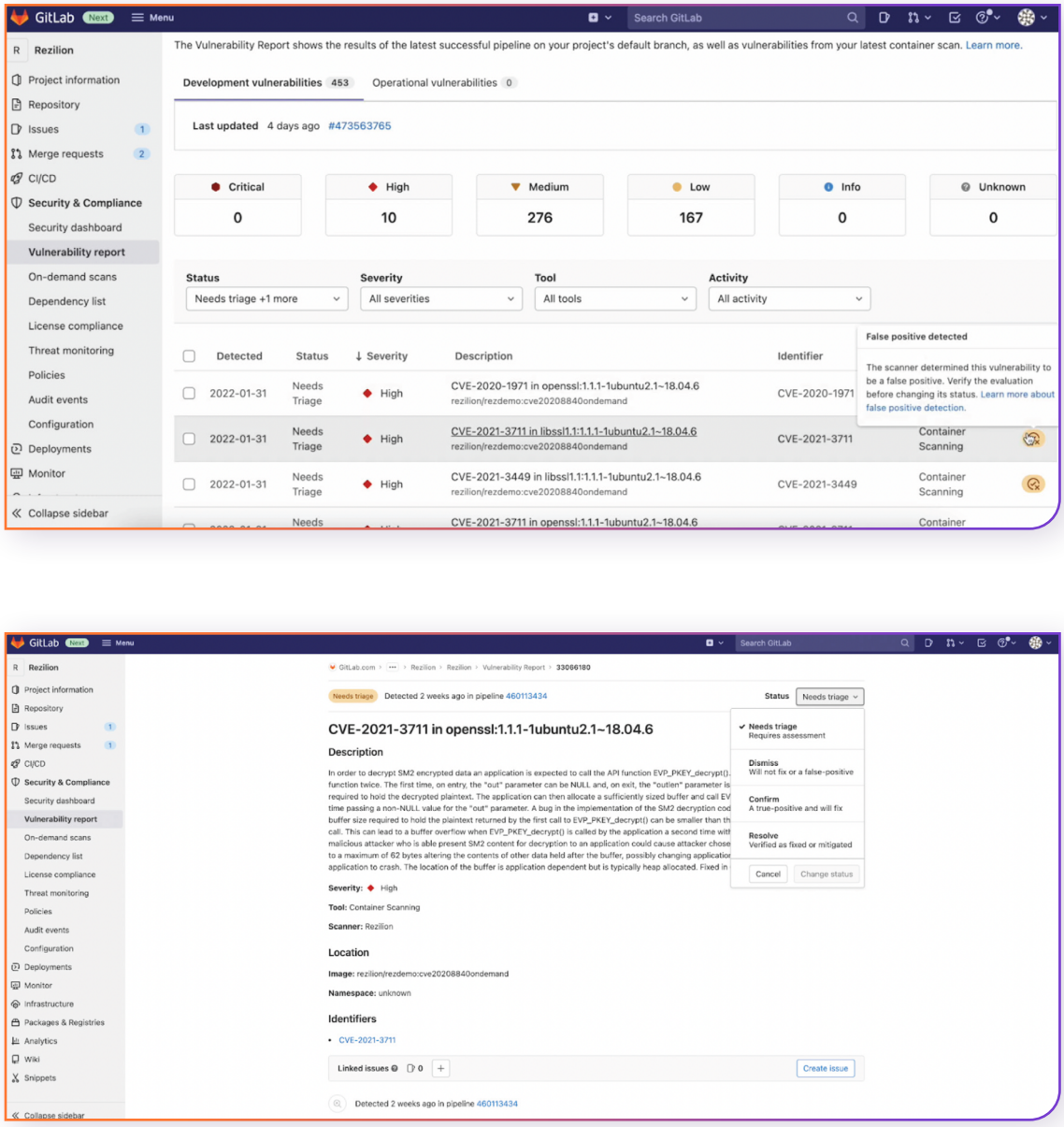

Figure 1: The vulnerability report shows a list of vulnerabilities in the customer's pipeline and marks them false positives. Additionally, each row shows when it was detected, its status, severity, and details.

VALIDATED VULNERABILITIES

CVE ID	Severity	Description	State
CVE-2020-27350	Medium	APT had several integer overflows and underflows while parsing .deb packages, aka GHSL-2020-168 GHSL-2020-169, in files apt-pkg/contrib/extracttar.cc, apt-pkg/deb/debfile.cc, and apt-pkg/contrib/arfile.cc. This issue affects: apt 1.2.32ubuntu0 versions prior to 1.2.32ubuntu0.2; 1.6.12ubuntu0 versions prior to 1.6.12ubuntu0.2; 2.0.2ubuntu0 versions prior to 2.0.2ubuntu0.2; 2.1.10ubuntu0 versions prior to 2.1.10ubuntu0.1;	Exploitable
CVE-2019-18276	Low	An issue was discovered in disable_priv_mode in shell.c in GNU Bash through 5.0 patch 11. By default, if Bash is run with its effective UID not equal to its real UID, it will drop privileges by setting its effective UID to its real UID. However, it does so incorrectly. On Linux and other systems that support "saved UID" functionality, the saved UID is not dropped. An attacker with command execution in the shell can use "enable -f" for runtime loading of a new builtin, which can be a shared object that calls setuid() and therefore regains privileges. However, binaries running with an effective UID of 0 are unaffected.	Exploitable
CVE-2018-7738	Low	In util-linux before 2.32-rc1, bash-completion/umount allows local users to gain privileges by embedding shell commands in a mountpoint name, which is mishandled during a umount command (within Bash) by a different user, as demonstrated by logging in as root and entering umount followed by a tab character for autocompletion.	Unexploitable
CVE-2016-2781	Low	chroot in GNU coreutils, when used with --userspec, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.	Exploitable
CVE-2020-8285	Medium	curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard match parsing.	Unexploitable
CVE-2020-8286	Medium	curl 7.41.0 through 7.73.0 is vulnerable to an improper check for certificate revocation due to insufficient verification of the OCSP response.	Unexploitable
CVE-2021-22876	Medium	curl 7.1.1 to and including 7.75.0 is vulnerable to an "Exposure of Private Personal Information to an Unauthorized Actor" by leaking credentials in the HTTP Referer: header. libcurl does not strip off user credentials from the URL when automatically populating the Referer: HTTP request header field in outgoing HTTP requests, and therefore risks leaking sensitive data to the server that is the target of the second HTTP request.	Unexploitable
CVE-		libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse, if one of them matches the setup.Due to errors in the logic, the config matching function did not take 'issuercert' into account and it compared the involved	

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

VULNERABLE COMPONENTS

Package Name	Package Version	Package Type	Highest Severity	State	Evidence
apt	1.6.12ubuntu0.1	Debian	Medium	Unsupported	
bash	4.4.18-2ubuntu1.2	Debian	Low	Exploitable	Loaded Files: /bin/bash
bsdutils	1:2.31.1-0.4ubuntu3.6	Debian	Low	Unexploitable	
coreutils	8.28-1ubuntu1	Debian	Low	Exploitable	Loaded Files: /bin/sleep,/usr/bin/timeout
curl	7.58.0-2ubuntu3.9	Debian	Medium	Unexploitable	
dbus	1.12.2-1ubuntu1.2	Debian	Low	Unsupported	
fdisk	2.31.1-0.4ubuntu3.6	Debian	Low	Unexploitable	
gcc-8-base	8.4.0-1ubuntu1~18.04	Debian	Medium	Unexploitable	
gpgv	2.2.4-1ubuntu1.2	Debian	Low	Unexploitable	
krb5-locales	1.16-2ubuntu0.1	Debian	Medium	Unexploitable	
libapparmor1	2.12-4ubuntu5.1	Debian	Medium	Unexploitable	
libapt-pkg5.0	1.6.12ubuntu0.1	Debian	Medium	Unexploitable	
libasn1-8-heimdal	7.5.0+dfsg-1	Debian	Low	Unexploitable	
libavahi-client3	0.7-3.1ubuntu1.2	Debian	Medium	Unexploitable	
libavahi-common-data	0.7-3.1ubuntu1.2	Debian	Medium	Unexploitable	
libavahi-common3	0.7-3.1ubuntu1.2	Debian	Medium	Unexploitable	

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

SBOM

CVE ID	Severity	Description	State
CVE-2020-27350	Medium	APT had several integer overflows and underflows while parsing .deb packages, aka GHSL-2020-168 GHSL-2020-169, in files apt-pkg/contrib/extracttar.cc, apt-pkg/deb/debfile.cc, and apt-pkg/contrib/arfile.cc. This issue affects: apt 1.2.32ubuntu0 versions prior to 1.2.32ubuntu0.2; 1.6.12ubuntu0 versions prior to 1.6.12ubuntu0.2; 2.0.2ubuntu0 versions prior to 2.0.2ubuntu0.2; 2.1.10ubuntu0 versions prior to 2.1.10ubuntu0.1;	Exploitable
CVE-2019-18276	Low	An issue was discovered in disable_priv_mode in shell.c in GNU Bash through 5.0 patch 11. By default, if Bash is run with its effective UID not equal to its real UID, it will drop privileges by setting its effective UID to its real UID. However, it does so incorrectly. On Linux and other systems that support "saved UID" functionality, the saved UID is not dropped. An attacker with command execution in the shell can use "enable -f" for runtime loading of a new builtin, which can be a shared object that calls setuid() and therefore regains privileges. However, binaries running with an effective UID of 0 are unaffected.	Exploitable
CVE-2018-7738	Low	In util-linux before 2.32-rc1, bash-completion/umount allows local users to gain privileges by embedding shell commands in a mountpoint name, which is mishandled during a umount command (within Bash) by a different user, as demonstrated by logging in as root and entering umount followed by a tab character for autocompletion.	Unexploitable
CVE-2016-2781	Low	chroot in GNU coreutils, when used with --userspec, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.	Exploitable
CVE-2020-8285	Medium	curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard match parsing.	Unexploitable
CVE-2020-8286	Medium	curl 7.41.0 through 7.73.0 is vulnerable to an improper check for certificate revocation due to insufficient verification of the OCSP response.	Unexploitable
CVE-2021-22876	Medium	curl 7.1.1 to and including 7.75.0 is vulnerable to an "Exposure of Private Personal Information to an Unauthorized Actor" by leaking credentials in the HTTP Referer: header. libcurl does not strip off user credentials from the URL when automatically populating the Referer: HTTP request header field in outgoing HTTP requests, and therefore risks leaking sensitive data to the server that is the target of the second HTTP request.	Unexploitable
CVE-		libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse, if one of them matches the setup.Due to errors in the logic, the config matching function did not take 'issuercert' into account and it compared the involved	

Figure 4: The dynamic SBOM shows all software components present in your environment.

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.

Please contact us for your free 30 day trial here.