ActiveState

Enterprise-Wide Vulnerability Dashboard

Software developers have long deployed tools and processes to ensure they have visibility into the open source dependencies they use. Unfortunately, too many organizations track only top-level packages, and may not have visibility into the complete list of transitive dependencies those packages are pulling in.

Additionally, enterprises may have visibility on a per business unit basis, but lack an automated way to determine organization-wide risk posed by a vulnerability, making prioritization and triage more difficult.

It's these kinds of blind spots that generate unnecessary risk, and can only be overcome by implementing a vulnerability dashboard that eliminates silos and identifies vulnerabilities across the extended enterprise, down to the lowest-level transitive dependency.

Open Source Observability

Open source observability starts with a comprehensive catalog of all dependencies, transitive dependencies and shared libraries for all software assets, no matter where they're deployed across the extended enterprise.

But with organizations increasing their use of open source components, the number of vulnerabilities being reported has exploded, resulting in ever-escalating risk due to:

- Hackers exploiting economies of scale: a single compromised open source package incorporated into a popular software application can allow them to potentially hack thousands of customers.
- 80% of codebases never being updated for fear of breaking the build, which leads to applications riddled with open source vulnerabilities.

These trends are exacerbated by silos, whereby:

- Each project may have different methods of obtaining the open source resources they require, including risky processes like downloading prebuilt, unsigned packages or source code from public repositories.
- Even when all open source artifacts are built from source code, they may be built on an unsecured developer desktop rather than a hardened build service.
- Open source components may be deployed on a project to project basis from a variety of prebuilt distributions that quickly become out of date.

The impact of silos both within a business unit and across the extended enterprise impacts risk assessment, prioritization and remediation. Multiple disparate tools and processes will lead to inconsistent and incomplete views of vulnerabilities, making it difficult to accurately assess risk, prioritize efforts, and remediate issues.

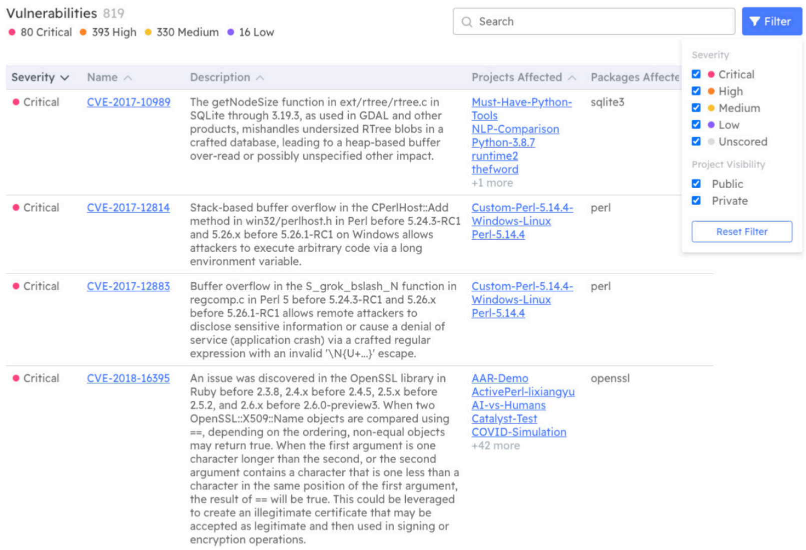
ActiveState CVE Dashboard

Open source observability is key to breaking down silos and reducing security risk, which means all stakeholders need to be able to visualize:

- The complete list of dependencies in use across the organization, including all transitive dependencies, shared libraries and OS-native binaries.
- Where each set of dependencies is deployed across the extended enterprise.

The ActiveState Vulnerability Dashboard is designed to do just that by providing a comprehensive view of dependencies and their vulnerabilities, enabling more effective risk assessment and remediation efforts.

It also allows security teams to regain control over proliferating projects and the open source dependencies they include by providing a single, central view of all open source runtime environments created for use:



Vulnerabilities 819

● 80 Critical ● 393 High ● 330 Medium ● 16 Low

Severity
☑ ● Critical
☑ ● High
☑ ● Medium
☑ ● Low
☑ ● Unscored

Project Visibility
☑ Public
☑ Private

Severity	Name	Description	Projects Affected	Packages Affecte
● Critical	CVE-2017-10989	The getNodeSize function in ext/rtree/rtree.c in SQLite through 3.19.3, as used in GDAL and other products, mishandles undersized RTree blobs in a crafted database, leading to a heap-based buffer over-read or possibly unspecified other impact.	Must-Have-Python-Tools NLP-Comparison Python-3.8.7 runtime2 thefword +1 more	sqlite3
● Critical	CVE-2017-12814	Stack-based buffer overflow in the CPerlHost::Add method in win32/perlhost.h in Perl before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 on Windows allows attackers to execute arbitrary code via a long environment variable.	Custom-Perl-5.14.4-Windows-Linux Perl-5.14.4	perl
● Critical	CVE-2017-12883	Buffer overflow in the S_grok_bslash_N function in regcomp.c in Perl 5 before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to disclose sensitive information or cause a denial of service (application crash) via a crafted regular expression with an invalid '\N{U+...}' escape.	Custom-Perl-5.14.4-Windows-Linux Perl-5.14.4	perl
● Critical	CVE-2018-16395	An issue was discovered in the OpenSSL library in Ruby before 2.3.8, 2.4.x before 2.4.5, 2.5.x before 2.5.2, and 2.6.x before 2.6.0-preview3. When two OpenSSL::X509::Name objects are compared using ==, depending on the ordering, non-equal objects may return true. When the first argument is one character longer than the second, or the second argument contains a character that is one less than a character in the same position of the first argument, the result of == will be true. This could be leveraged to create an illegitimate certificate that may be accepted as legitimate and then used in signing or encryption operations.	AAR-Demo ActivePerl-lixiangyu AI-vs-Humans Catalyst-Test COVID-Simulation +42 more	openssl

- Visualize the security status of every project
- Filter by severity
- Search for specific CVEs
- At-a-glance view of number of affected projects, facilitating triage
- Comprehensive list of affected dependencies, including all transitive dependencies

Uniquely, security teams can Immediately update projects with newer (fixed) versions of vulnerable packages, automatically rebuild the runtime environment ready for testing, and thereby decrease Mean Time To Remediation (MTTR).

About ActiveState

ActiveState is the de-facto standard for millions of developers around the world who have been using our commercially-backed, secure open source language distributions for over 20 years. With the ActiveState Platform, developers can now automatically build their own open source artifacts and environments—all without requiring language or operating system expertise.

You can try the ActiveState Platform by signing up for a free account at **platform.activestate.com**

ActiveState

www.activestate.com
Toll-free in NA: 1-866.631.4581
solutions@activestate.com