ActiveState

Open Source Observability

Breaking Down Security Silos

Pete Garcin and Evan Smith

Housekeeping

- We will host 2 polls during the webinar
- You will receive an email with the recording
- Submit your questions in the Q&A tab and we’ll address them at the end, so stick with us!

Introductions

Pete Garcin

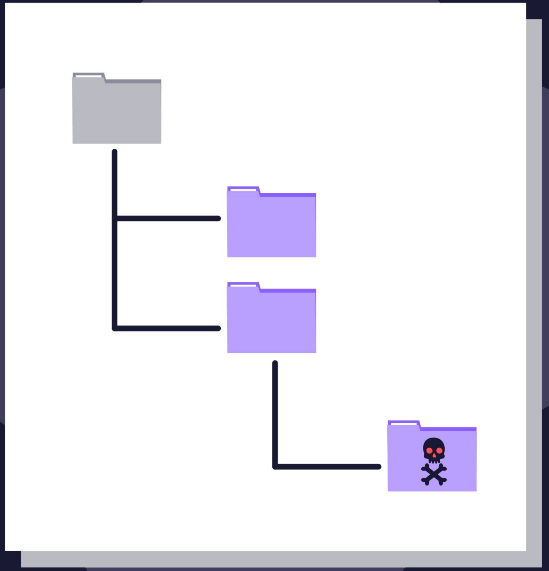
Director of Product,
ActiveState

Evan Smith

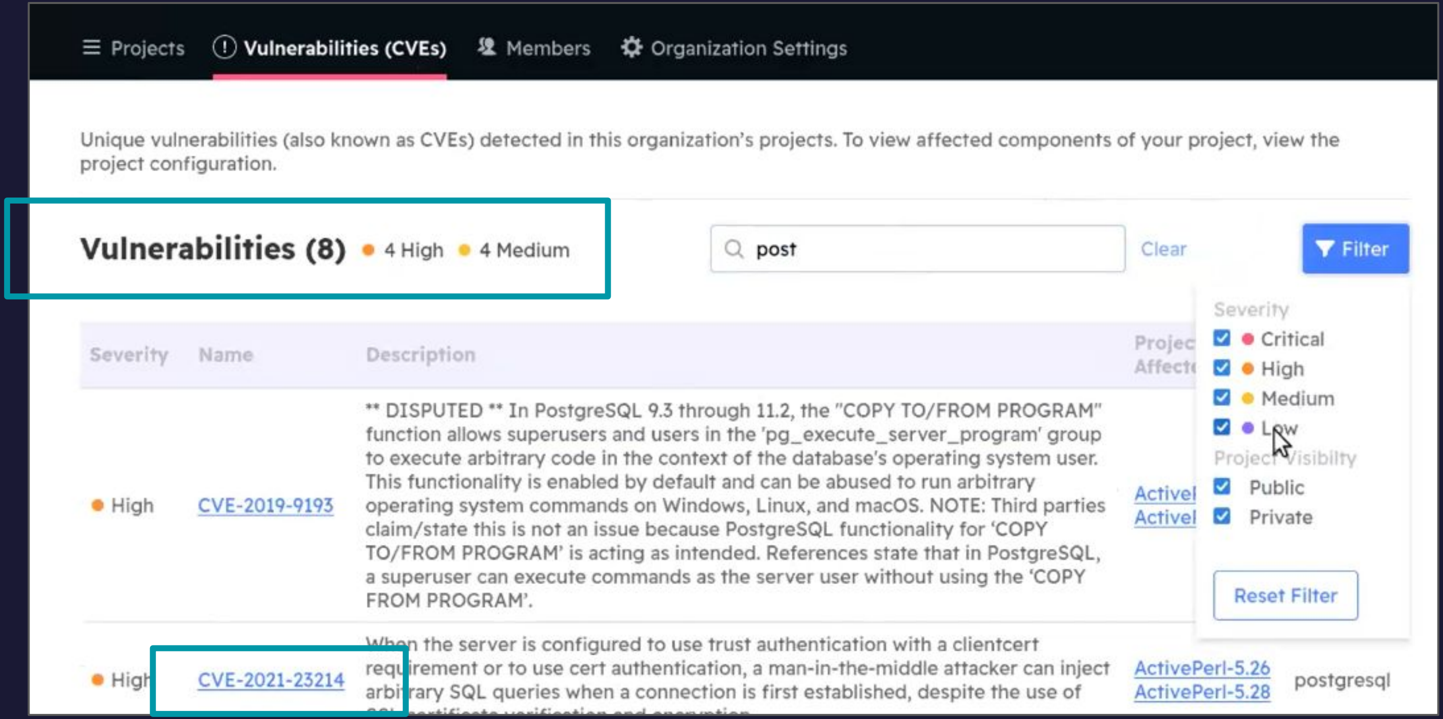
Director of Customer Success,
ActiveState

ActiveState

ActiveState



Achieving Open Source Observability



Unique vulnerabilities (also known as CVEs) detected in this organization's projects. To view affected components of your project, view the project configuration.

Vulnerabilities (8) ● 4 High ● 4 Medium

post

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

Project Visibility
☑ Public
☑ Private

Severity	Name	Description	Projec Affecte	
● High	CVE-2019-9193	** DISPUTED ** In PostgreSQL 9.3 through 11.2, the "COPY TO/FROM PROGRAM" function allows superusers and users in the 'pg_execute_server_program' group to execute arbitrary code in the context of the database's operating system user. This functionality is enabled by default and can be abused to run arbitrary operating system commands on Windows, Linux, and macOS. NOTE: Third parties claim/state this is not an issue because PostgreSQL functionality for 'COPY TO/FROM PROGRAM' is acting as intended. References state that in PostgreSQL, a superuser can execute commands as the server user without using the 'COPY FROM PROGRAM'.	ActiveI ActiveI	
● High	CVE-2021-23214	When the server is configured to use trust authentication with a clientcert requirement or to use cert authentication, a man-in-the-middle attacker can inject arbitrary SQL queries when a connection is first established, despite the use of SSL certificate verification and encryption.	ActivePerl-5.26 ActivePerl-5.28	postgresql

Poll:

What is your current level of observability? (Check one)

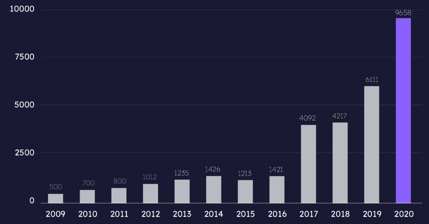
We know about vulnerabilities in:

- ■ Nothing, we don’t have any visibility
- ■ Only our top-level (ie. direct) open source dependencies
- ■ All layers of open source dependencies (ie. including transitive)
- ■ All of the above plus we have provenance and a secure build process
- ■ Don’t know

Why is Supply Chain Security Tough?

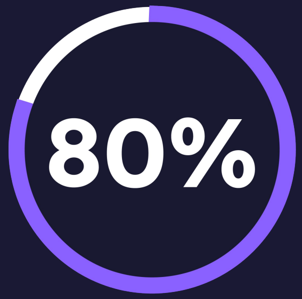
The landscape of open source vulnerabilities

Open Source Vulnerabilities per Year: 2009-2020



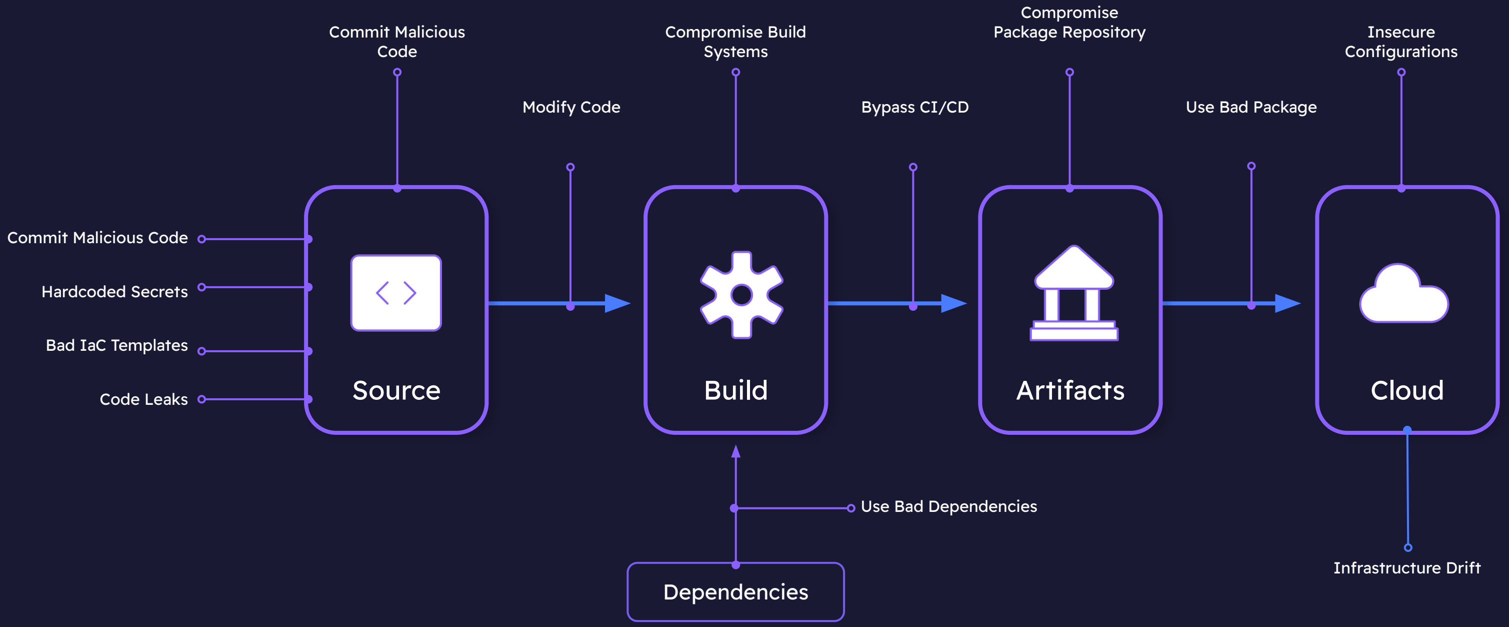
The challenge of visibility in open source

Codebase updates just don't happen

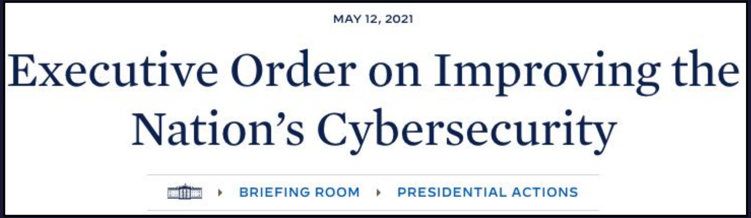


ActiveState

Open Source Vulnerabilities and the Software Supply Chain



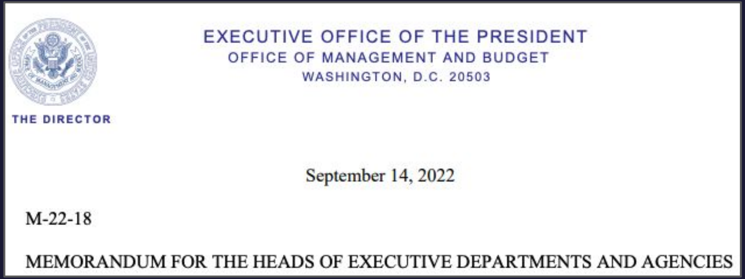
US Executive Order on Vulnerability Remediation



MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

▸ BRIEFING ROOM ▸ PRESIDENTIAL ACTIONS



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

September 14, 2022

M-22-18

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SECURING THE SOFTWARE SUPPLY CHAIN

RECOMMENDED PRACTICES GUIDE FOR DEVELOPERS

Silos and Security Checkpoints

Source:

first party code
code review
source control

Build:

Build platform,
CI/CD,
artifact repository

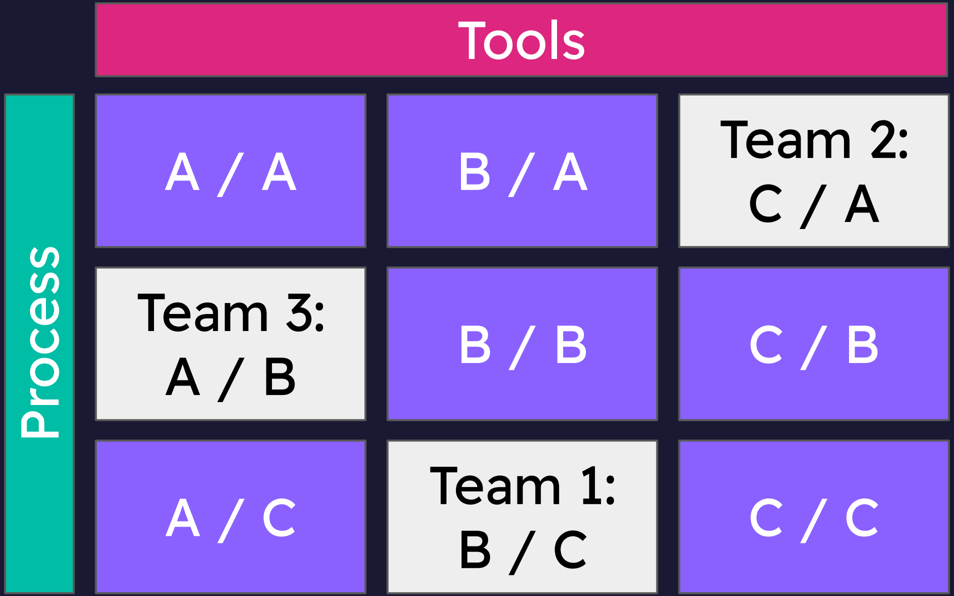
Dependency:

compromised
dependency

Deployment Threats:

deployment process, noncompliance,
vulnerabilities

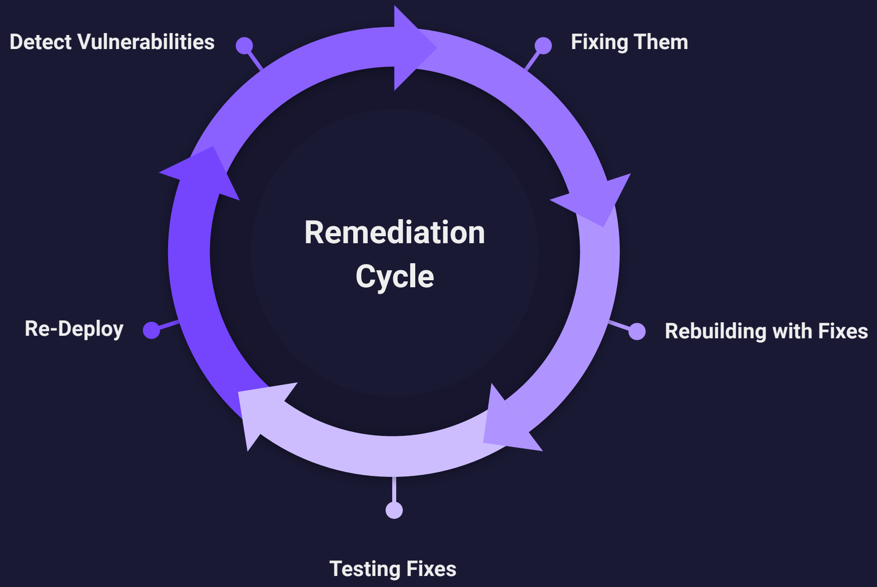
Combinatorial Explosions of Complexity



	Tools		
Process	A / A	B / A	Team 2: C / A
	Team 3: A / B	B / B	C / B
	A / C	Team 1: B / C	C / C

- Even with 3 disparate process and 3 tools things get quickly complicated
- How could a CISO tell who is doing what, when?
- How can groups observe each other’s outputs or processes cleanly?

Accelerating the Remediation Cycle

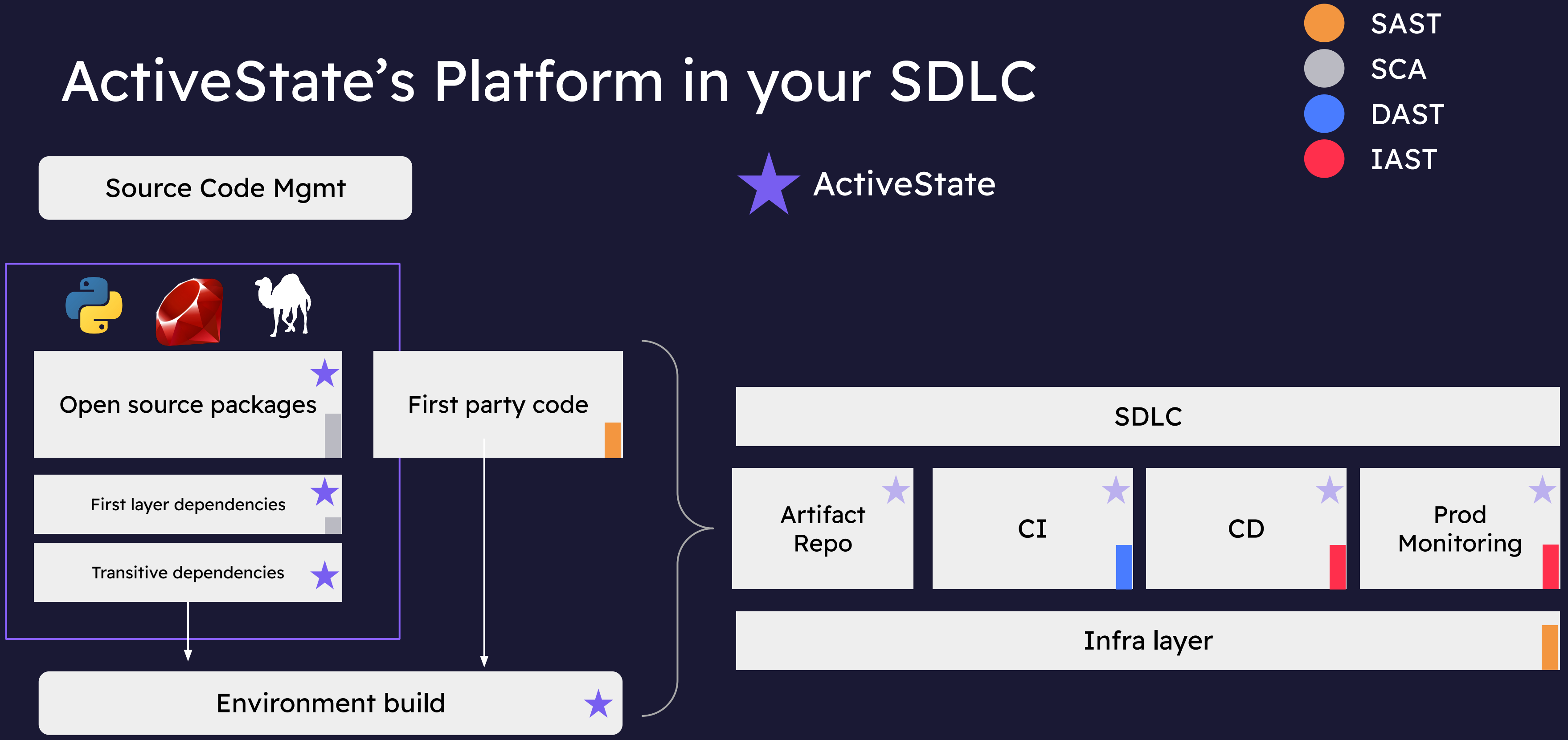


Poll:

How long does it currently take to remediate a vulnerability? (Check one)

- ■ A few hours
- ■ A few days or weeks
- ■ 1-2 months
- ■ 2-5 months
- ■ 5+ months
- ■ Don’t know

ActiveState's Platform in your SDLC



Scenario: DevSec sends an email about two pressing issues

- Latest **tensorflow** must be used, no other versions of tensorflow are allowed.

- Please report any use of **wheel**.

  CVE-2022-40898
  https://nvd.nist.gov/vuln/detail/CVE-2022-40898

  An issue discovered in Python Packaging Authority (PyPA) Wheel 0.37.1 and earlier allows remote attackers to cause a denial of service via attacker controlled input to wheel cli.

Project Examples

1. just-tensorflow

Top level requirements:

- tensorflow

2. what-wheel

Top level requirements:

- boost
- bottle
- keras
- numpy
- requests
- tables

How can these issues be addressed?

Option 1

Self Remediation

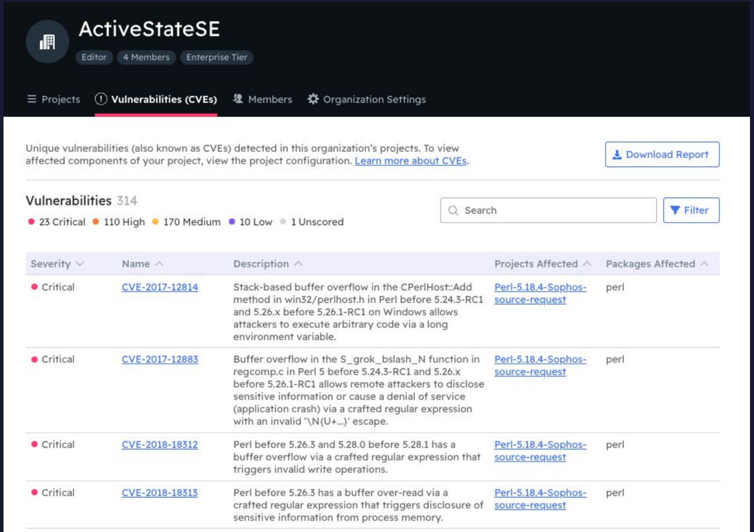
Dear DevSec,
Everything is fine.

Sincerely,

Nothing to Worry About

Option 2

ActiveState Platform



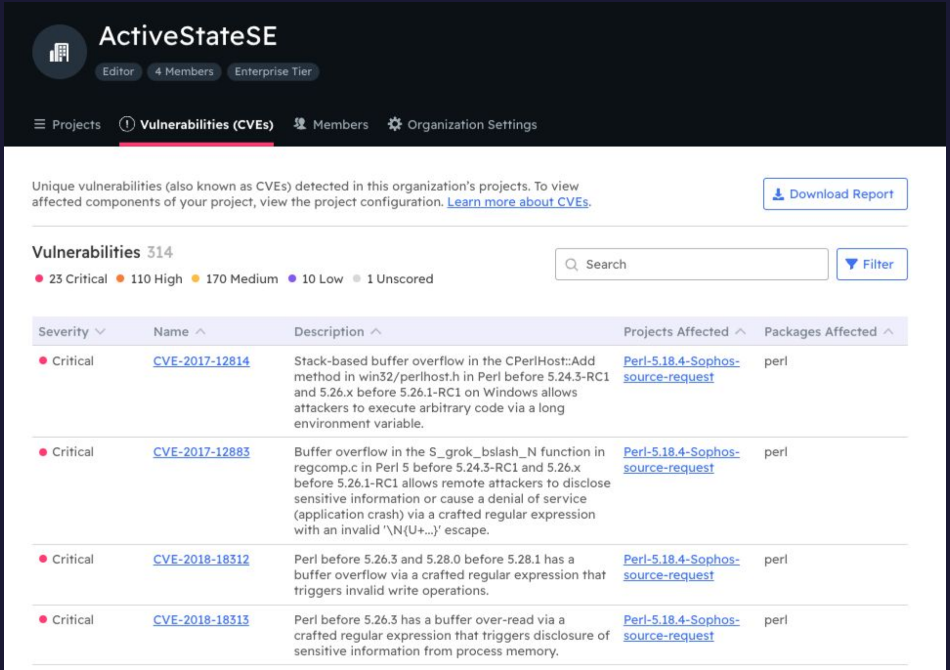
Unique vulnerabilities (also known as CVEs) detected in this organization's projects. To view affected components of your project, view the project configuration. Learn more about CVEs.

Vulnerabilities 314

● 23 Critical ● 110 High ● 170 Medium ● 10 Low ● 1 Unscored

Severity	Name	Description	Projects Affected	Packages Affected
● 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.	Perl-5.18.4-Sophos-source-request	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.	Perl-5.18.4-Sophos-source-request	perl
● Critical	CVE-2018-18312	Perl before 5.26.3 and 5.28.0 before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.	Perl-5.18.4-Sophos-source-request	perl
● Critical	CVE-2018-18313	Perl before 5.26.3 has a buffer over-read via a crafted regular expression that triggers disclosure of sensitive information from process memory.	Perl-5.18.4-Sophos-source-request	perl

ActiveState Platform



Unique vulnerabilities (also known as CVEs) detected in this organization's projects. To view affected components of your project, view the project configuration. Learn more about CVEs.

Vulnerabilities 314

● 23 Critical ● 110 High ● 170 Medium ● 10 Low ● 1 Unscored

Severity	Name	Description	Projects Affected	Packages Affected
● 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.	Perl-5.18.4-Sophos-source-request	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.	Perl-5.18.4-Sophos-source-request	perl
● Critical	CVE-2018-18312	Perl before 5.26.3 and 5.28.0 before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.	Perl-5.18.4-Sophos-source-request	perl
● Critical	CVE-2018-18313	Perl before 5.26.3 has a buffer over-read via a crafted regular expression that triggers disclosure of sensitive information from process memory.	Perl-5.18.4-Sophos-source-request	perl

Q&A

Thanks for Joining Us!

Get our Journey to Supply Chain Security eBook:

https://www.activestate.com/resources/white-papers/the-journey-to-software-supply-chain-security/

Try the ActiveState Platform:

https://platform.activestate.com/

Join Our Early Access Program

Try our Security Dashboard and gain visibility of vulnerabilities across your organization!