ANACONDA

# Go Beyond Basic Vulnerability Data With Anaconda

Anaconda's curated vulnerability data enables you to focus on the vulnerabilities that matter most to you.

## What Are CVEs?

CVEs, short for Common Vulnerabilities and Exposures, are security flaws that have been publicly disclosed, typically by way of the National Institute of Standards and Technology (NIST). These CVEs are made available by NIST through the National Vulnerability Database (NVD), which is the U.S. government repository of vulnerability data.

Thousands of CVEs are issued each year, and each one may represent a potential opening for a cyberattack.

## How Is Anaconda's CVE Data Different?

Are you relying on scanning tools or manual processes to identify and vet every CVE? Up to 75% of vulnerability alerts are false positives, resulting in months of wasted time spent trying to verify details and implement fixes.

Anaconda analyzes each vulnerability associated with packages in our repository, assigning one of five labels:

| Reported | Active | Cleared | Mitigated | Disputed |
|---|---|---|---|---|
| All CVEs that come from NIST | Vulnerabilities that are still potentially active | Vulnerabilities that have been analyzed and determined not to be applicable | Vulnerabilities that were proactively mitigated with a code patch | Vulnerabilities that were disputed by upstream project maintainers or other community members |

This enables our customers to focus on identifying and remediating only the CVEs that matter most.

## Why Anaconda?

Organizations have a security gap when it comes to their open-source data science pipelines. Most security tools on the market work well for DevOps and languages such as JavaScript, but are not ideal for Python.

As the curators and maintainers of the Anaconda repository, we are deeply familiar with the Python and R open-source ecosystem and compile all packages according to our own build and test standards. Not only do we provide you with the pertinent CVE data, we also provide tools that leverage this data to block vulnerable packages upstream of your open-source pipeline, securing your organization's software supply chain.

Our products secure open-source pipelines at world-class organizations such as Nissan, MetLife, Danske Bank, and others.

## Why Now?

The frequency and cost of cyberattacks is increasing. 2021 saw a 650% increase in cyberattacks aimed at open source, with an average cost of $1.4 million to remediate a single ransomware attack.

Organizations cannot afford to ignore these risks, but managing this process manually is expensive and time consuming. With thousands of new CVEs introduced each year alongside ongoing updates, organizations can typically only manage a small subset of all the open-source software (OSS) actually being utilized.

Anaconda's curated CVE data is comprehensive and actionable, potentially saving countless hours of manual vetting and substantial costs related to managing the process in-house.

## Anaconda CVE Curation vs. Public Data

**What does Anaconda's curated CVE data look like in action?**

A security scan of the OSS in an organization's pipeline typically results in a list of alerts, letting you know that several packages have associated vulnerabilities. Investigating these alerts may take anywhere from one hour to several days. Oftentimes, the result of such an investigation is learning that the upstream maintainer has already implemented a patch, or the vulnerability applies to a little-used function of the package, and so on. In these cases, the vulnerability isn't actually a threat anymore, but organizations still must invest significant time in order to verify this. This ultimately leads to developers and IT managers getting alert fatigue.

This ultimately leads to developers and IT managers getting alert fatigue. There are simply too many alerts and false alarms, so they stop paying as much attention, opening the door for a real threat to slip through the cracks. It can be difficult to discern which CVEs need attention and which are not relevant. The public databases have no mechanism for discerning this, which is where Anaconda's curation can help.

In this situation, a company using Anaconda's curated CVE metadata could sort out the real risk in a few minutes, versus the hours or days it may take to verify this information manually. Anaconda's curation team manually reviews flagged packages from the NVD, verifies what software the CVE affects, and curates a CVE status that saves IT teams from countless hours of manual vetting.

## Here are a few examples of Anaconda CVE curation at work:

| CVE | CVE-2019-10128 | CVE-2016-1906 | Multiple |
|---|---|---|---|
| Details | Critical CVE associated with PostgreSQL | Critical CVE associated with Python Kubernetes project | CVEs associated with ICU 58.2 patches were provided by upstream maintainer |
| Curation | Verified Anaconda packages do not use the vulnerable component | Discovered incorrect association—vulnerability actually impacted Kubernetes server product | Applied patches to Anaconda packages |
| Result | CLEARED<br>👍 | CLEARED<br>👍 | MITIGATED<br>🛡 |

## To secure your open-source software with Anaconda's curated vulnerability data, reach out to sales@anaconda.com.

With more than 35 million users, Anaconda is the world's most popular platform to develop and deploy secure Python solutions, faster. We pioneered the use of Python for data science, champion its vibrant community, and steward the open-source projects behind tomorrow's artificial intelligence (AI) and machine learning (ML) breakthroughs. Our solutions enable practitioners and institutions around the world to securely harness the power of open source for competitive advantage and groundbreaking discoveries.

**Visit Anaconda.com to learn more.**