Trend Micro Cloud One™ – Open Source Security by Snyk

Visibility and tracking of open source vulnerabilities and license risks built for SecOps

Table of contents

››› Back to TOP

Purpose of This Guide:

Security practitioners will be given insight into the value of identifying and tracking the risks introduced by the use of open source components across their software development life cycle (SDLC). Aside from providing a better understanding of this growing threat landscape, this guide will outline the importance of protecting business processes and corporate assets. Methods to mitigate vulnerabilities in open source components, used by the organization's custom-built applications, will also be explored. Use this guide to learn more about Trend Micro Cloud One™ – Open Source Security by Snyk and how to get started.

The Rise of Open Source

As the demand for web, mobile, and cloud-native applications increases across business and consumer requirements, so has the use of open source software. Well-designed open source libraries help speed up development cycles for commercial software by providing components that reduce the need to build entire applications from the bottom up. Open source libraries provide a significant advantage due to public availability, ease-of-use, and decentralization abilities for modern software development.

Yet, as with any software, there are potential security risks. Vulnerabilities can sometimes go unchecked because organizations are unaware that they are using a vulnerable open source component in their application. While the open source community can identify potential exploits and report them to be fixed, bad actors can also scour code or take advantage of publicly available vulnerability listings that can affect millions of projects.

What Are Open Source Vulnerabilities?

Introduced through open source components that contain weaknesses in the code, open source vulnerabilities are capabilities that can be exploited by an attacker—introduced accidentally as a bug or added intentionally in specially crafted malicious packages. In addition, open source software can unexpectedly cause license risks for the organization as these components allow developers and users to view, modify, and distribute the software to anyone for any purpose. This practice is common due to the majority of open source software being worked on and distributed in a collaborative public process.

> "Open source software is used within mission-critical IT workloads by over 95% of the IT organizations worldwide, whether they are aware or not"
>
> - Gartner Market Guide for Software Composition Analysis [1]

[1] Gartner Market Guide for Software Composition Analysis, 18 August 2020- ID G00721255

››› Back to TOP

What Should CISOs Consider?

Organizations are increasingly more aware of the impact open source risks can have on upstream processes and their overall security posture. However, maintaining necessary visibility across multiple development teams, regions, and projects has proved to be a daunting task.

CISOs need to consider that building applications on open source libraries requires pulling in a great number of dependencies, which can increase risks organizations face from both security and a license compliance standpoints.

> “75% of codebases audited by security vendors had security vulnerabilities or license risks.”
>
> - Snyk State of Open Source Security Report[2]

Cloud computing uses source components that often create blind spots for security operations teams. Unfortunately, some security practices and tools do not provide visibility or robust Software Composition Analysis (SCA) into the security risks present in open source library dependency. Security teams, as well as business and legal teams, can be overwhelmed with developer-focused detail that lacks the language needed to identify and monitor security and license risks.

Deployed applications bundle your proprietary code and selected open source code along with your dependencies. Keeping track of all libraries and dependencies requires time despite being an important critical task. Many traditional tools are not able to dig deeper into indirect or transitive dependencies and lack well-architected dependency trees to help SecOps define risks.

> “78% of vulnerabilities are found in indirect dependencies”
>
> - Snyk State of Open Source Security Report[3]

[2] Snyk State of Open Source Security Report, April 2020
[3] Snyk State of Open Source Security Report, April 2020

››› Back to TOP

What Should Security Practitioners Consider?

Traditional code-base vulnerability detection solutions keep security teams siloed and don't allow SecOps to go from zero visibility to completely informed. Development teams have always had the ability to measure success through tools specific to their needs while security teams have been left out of the code vulnerability discussion within the SDLC.

Many organizations rely on Static Application Security Testing (SAST), or Dynamic Application Security Testing (DAST). These tools are critical when it comes to scanning for vulnerabilities in 'closed source' or proprietary code, however proprietary code in custom applications only make up a fraction of the code base itself and does not address open source components.

While proprietary code can be equally vulnerable—as demonstrated by the 2020 SolarWinds hack—it requires more effort and collaboration to find a vulnerability and is specific to a given application. Open source code vulnerabilities can be more easily exploited by the masses due to the fact that this code is publicized, available to test, and security databases list known-risks that may or may not have a patch. In addition, a single exploit of an open source vulnerability can be used to attack many organizations. Software composition analysis is agile across open source libraries as opposed to a specific code language or function.

When security tools don't easily integrate into developer workflows and CI/CD pipelines, it often results in a long list of nonactionable false-positives that hinder development. As security workflows and input shift further left, security teams and CISOs have less insight into the development pipeline, and protection accuracy and security depth can suffer.

While you have likely heard of DevSecOps methodologies and tools that attempt to close these gaps, many have created misalignment across toolsets and communication rifts between security and DevOps teams. As workflows shift left and DevOps teams gain momentum earlier in development, security operations teams still own risk management for their organizations.

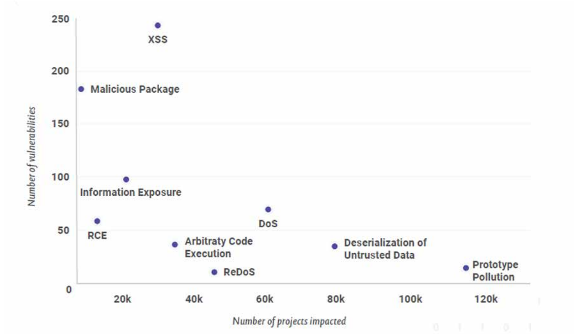
When security operations teams are able to successfully identify risks in open source code independently and manage up the open source security posture to the CISO, it's easier to collaborate with developers without impeding their workflows and efficiencies. This also makes it easier to gauge and forecast risk based on observing the open source detection over time and over its remediation progress.

››› Back to TOP

Open Source Risk Examples

Apache Struts is a free open source framework for creating Java web applications, widely used by Fortune 100 companies. Apache Struts2 exploit used against Equifax (CVE-2017-5638) was a result of Struts' parser, called Jakarta (responsible for the mismanagement of files uploaded to the web server) which allowed hackers to remotely run code.

A high severity prototype pollution security vulnerability (CVE-2019-10744) affected all versions of the popular "npm Lodash" library. The vulnerability could be exploited by an attacker to inject properties on "Object.prototype" to disclose or modify data or cause denial-of-service attacks. It was used by 4.35 million projects on GitHub alone. The project had just shy of 40k GitHub project stars, and the library had been downloaded over 80 million times each month.



In 2019, the popular npm ibrary Lodash was used by 4.35 million projects on GitHub alone. The project had just shy of 40k GitHub project stars, and the library had been downloaded over 80 million times each month.

Figure 1

Vulnerabilities Reported vs. Projects Impacted.[4]

An older example of an open source vulnerability is Heartbleed. Hundreds of millions of websites were affected in the popular OpenSSL cryptographic software library. This weakness allows bad actors to steal the information protected by the SSL/TLS encryption used to secure the internet (CVE-2014-0160).

Commercial software composition analysis (SCA solutions) goes beyond CVEs and curate their own databases with additional vulnerabilities and richer data, finding issues earlier, more accurately, while helping to fix them better. When using an SCA solution, check that its DB also tracks non-CVE vulnerabilities for maximum coverage.[5]

Some websites may depend on dozens or even hundreds of such libraries, which could be scattered across dozens of servers on multiple continents. Understanding that landscape quickly and holistically is critical to the security teams and business management. Having a keen sense of what is happening across all development teams is not easy, but it is possible and it can make a difference between being proactive and reactive to open source risks.

[4] Snyk State of Open Source Security Report, April 2020
[5] Securing Open Source Libraries, O'Reilly

››› Back to TOP

The Solution

As the IT landscape shifts more toward cloud-native application development, organizations need ongoing security visibility and tracking of open source vulnerabilities and license risk.

Development teams move fast, making it hard for SecOps to keep up. It becomes even more difficult when security teams are stretched thin and must oversee all business unit threats—those beyond the dozens of application development projects and code repositories. Security teams have worked hard to secure the stack by integrating both internal and external services protection. With the use of more open source components and the growth of DevOps, the security landscape has expanded, as has the attack surface.

It is critical to implement open source vulnerability detection into the security stack. This helps tighten security protocols and best practices further left in the software development life cycle. With SecOps having little influence at the code level, these teams can now have the visibility and awareness needed to make informed decisions and to track open source risks. This creates a better alliance and bridges the gap between SecOps and DevOps. Expert advice is given to security teams to help monitor and track risks throughout the software supply chain, providing protection and awareness early without being overlooked or neglected.

Organizations require solutions that can enable cohesion between development and security. This allows teams to efficiently manage and mitigate the risk introduced from the rapid pace of open source application development. To scale at a rapid pace, solutions must support development and security team alignment and close the communication and tool gap between one another.

Software Composition Analysis (SCA) is a solution built to help security teams surface vulnerabilities and license issues early in the development cycle. This enables security operations professionals to understand the known risk in their development projects and prioritize critical issues to fix.

Continuous insight and remediation into open source vulnerabilities and license issues in code unites developer and security operations teams.

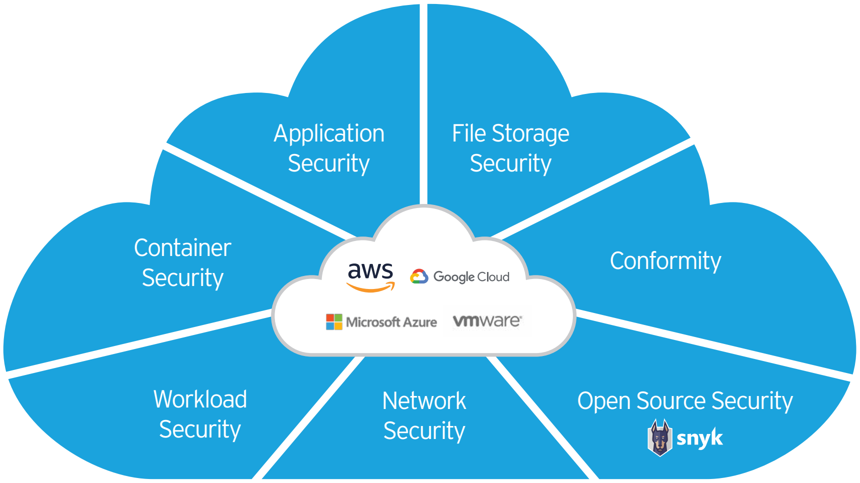
››› Back to TOP

Introducing Trend Micro Cloud One – Open Source Security by Snyk

The first-ever purpose-built service for security operations teams, Trend Micro Cloud One – Open Source Security by Snyk automatically finds, prioritizes, and reports vulnerabilities and license risks in open source dependencies used by your applications. As part of the Trend Micro Cloud One™ security platform, this solution connects with your code repositories and CI/CD pipelines to scan projects. Security teams are empowered with better visibility, tracking, and early awareness into open source issues.

Trend Micro Cloud One – Open Source Security by Snyk provides ongoing security insight to help organizations identify, manage, and resolve open source risks.

››› Back to TOP



Without visibility into open source code risks, the task of remediating vulnerabilities is an upstream process for security teams. At times, security teams can't move fast enough to keep pace with application development and require a systematic view into risks that can impact the business as well as its customers and partners. Trend Micro Cloud One – Open Source Security by Snyk delivers visibility into the overall state of the security compliance posture in one location, so SecOps can benefit from consolidated guidance and risk mitigation.

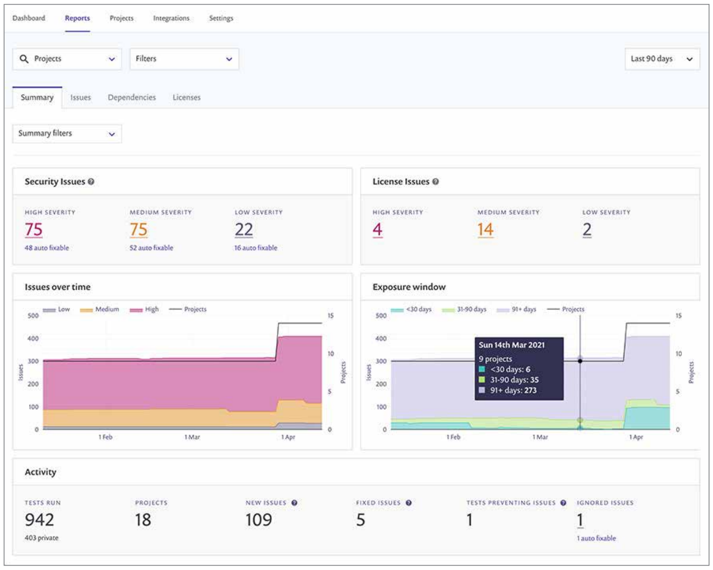
››› Back to TOP

Understanding How Trend Micro Can Help Reduce Open Source Risks

See all direct and indirect dependency paths to identify vulnerabilities in the open source code being used by your organization and receive clear details from the Knowledge Base on how to fix them.

Gain visibility

Scan projects in code repositories to gain visibility into open source dependency vulnerabilities. Monitor trends across your entire organization's open source landscape through dashboards and reports.



Security Issues

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
75	75	22
48 auto fixable	52 auto fixable	16 auto fixable

License Issues

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
4	14	2

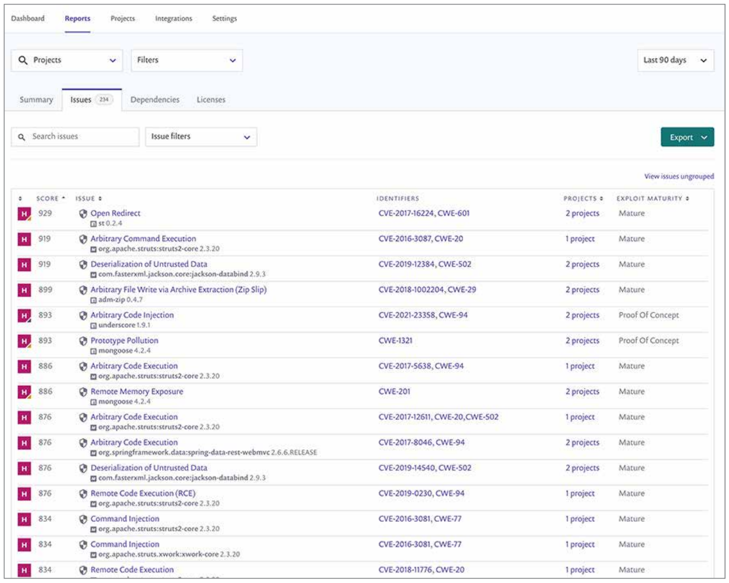
Sun 14th Mar 2021
9 projects
<30 days: 6
31-90 days: 35
91+ days: 273

Activity

TESTS RUN	PROJECTS	NEW ISSUES	FIXED ISSUES	TESTS PREVENTING ISSUES	IGNORED ISSUES
942 403 private	18	109	5	1	1 1 auto fixable

Eliminate blind spots

SecOps teams can generate an automated open source Bill of Materials report to immediately receive risk and priority scores to quickly deal with vulnerabilities and license issues. This includes zero-day threats detected early in the pipeline stages to ensure security awareness.

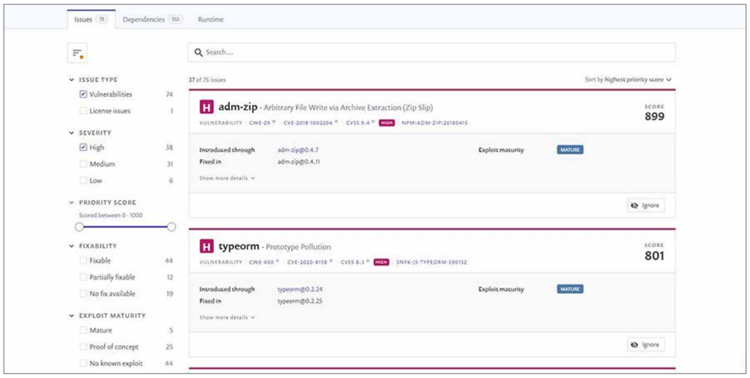


	SCORE	ISSUE	IDENTIFIERS	PROJECTS	EXPLOIT MATURITY
H	929	Open Redirect st 0.2.4	CVE-2017-16224, CWE-601	2 projects	Mature
H	919	Arbitrary Command Execution org.apache.struts:struts2-core 2.3.20	CVE-2016-3087, CWE-20	1 project	Mature
H	919	Deserialization of Untrusted Data com.fasterxml.jackson.core:jackson-databind 2.9.3	CVE-2019-12384, CWE-502	2 projects	Mature
H	899	Arbitrary File Write via Archive Extraction (Zip Slip) adm-zip 0.4.7	CVE-2018-1002204, CWE-29	2 projects	Mature
H	893	Arbitrary Code Injection underscore 1.9.1	CVE-2021-23358, CWE-94	2 projects	Proof Of Concept
H	893	Prototype Pollution mongoose 4.2.4	CWE-1321	2 projects	Proof Of Concept
H	886	Arbitrary Code Execution org.apache.struts:struts2-core 2.3.20	CVE-2017-5638, CWE-94	1 project	Mature
H	886	Remote Memory Exposure mongoose 4.2.4	CWE-201	2 projects	Mature
H	876	Arbitrary Code Execution org.apache.struts:struts2-core 2.3.20	CVE-2017-12611, CWE-20,CWE-502	1 project	Mature
H	876	Arbitrary Code Execution org.springframework.data:spring-data-rest-webmvc 2.6.6.RELEASE	CVE-2017-8046, CWE-94	2 projects	Mature
H	876	Deserialization of Untrusted Data com.fasterxml.jackson.core:jackson-databind 2.9.3	CVE-2019-14540, CWE-502	2 projects	Mature
H	876	Remote Code Execution (RCE) org.apache.struts:struts2-core 2.3.20	CVE-2019-0230, CWE-94	1 project	Mature
H	834	Command Injection org.apache.struts:struts2-core 2.3.20	CVE-2016-3081, CWE-77	1 project	Mature
H	834	Command Injection org.apache.struts.xwork:xwork-core 2.3.20	CVE-2016-3081, CWE-77	1 project	Mature
H	834	Remote Code Execution	CVE-2018-11776, CWE-20	1 project	Mature

>>> Back to TOP

Trusted security

Collaborate between SecOps and DevOps teams and establish best practices for open source use and accelerate remediation of cybersecurity risks. Use open source vulnerability details to correlate with those applications live in production.



Issues 75 | Dependencies 553 | Runtime

Search...

ISSUE TYPE
- ☑ Vulnerabilities 74
- ☐ License issues 1

SEVERITY
- ☑ High 38
- ☐ Medium 31
- ☐ Low 6

PRIORITY SCORE
Scored between 0 - 1000

FIXABILITY
- ☐ Fixable 44
- ☐ Partially fixable 12
- ☐ No fix available 19

EXPLOIT MATURITY
- ☐ Mature 5
- ☐ Proof of concept 25
- ☐ No known exploit 44

37 of 75 issues — Sort by highest priority score

H adm-zip - Arbitrary File Write via Archive Extraction (Zip Slip) — SCORE 899
VULNERABILITY | CWE-29 | CVE-2018-1002204 | CVSS 9.4 HIGH | NPM:ADM-ZIP:20180415
Introduced through adm-zip@0.4.7 — Exploit maturity MATURE
Fixed in adm-zip@0.4.11
Show more details
Ignore

H typeorm - Prototype Pollution — SCORE 801
VULNERABILITY | CWE-400 | CVE-2020-8158 | CVSS 8.3 HIGH | SNYK-JS-TYPEORM-590152
Introduced through typeorm@0.2.24 — Exploit maturity MATURE
Fixed in typeorm@0.2.25
Show more details
Ignore

Surface hidden license risks:

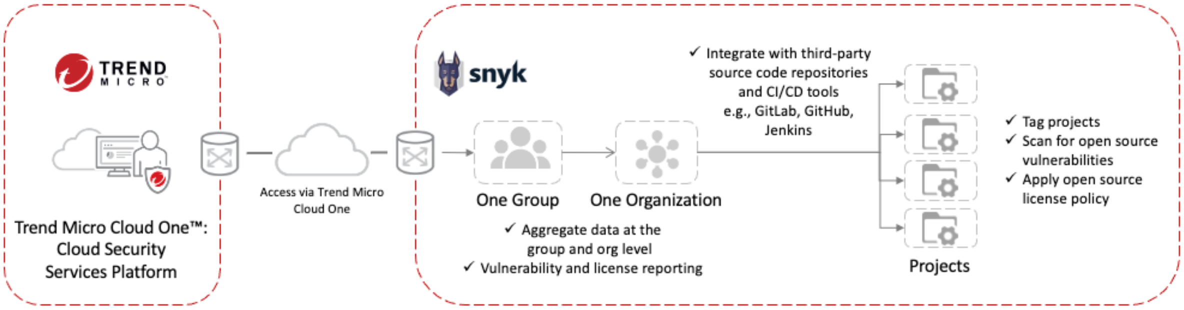
Security and Legal teams can benefit by receiving instructions about each license identified in your open source components and monitor them all from one place.

Complement existing services:

Increase protection across your security stack by including Trend Micro Cloud One™ – Container Security to gain deeper vulnerability detection at the container image and registry layer. Gain Kubernetes admission control and runtime protection and visibility into all applications.

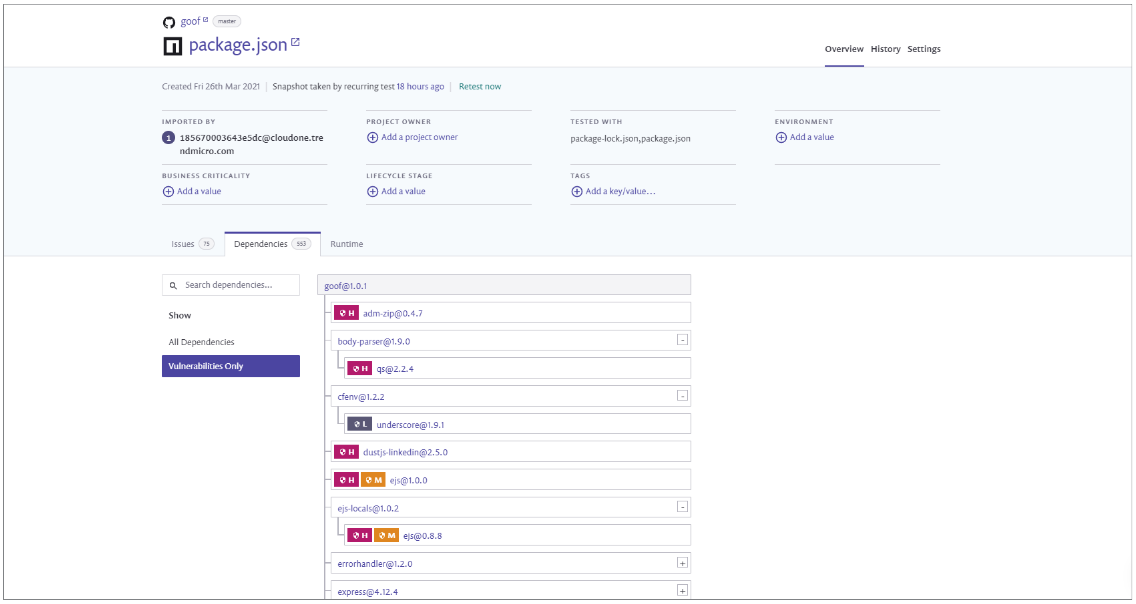
Trend Micro Cloud One™ – Open Source Security by Snyk

Trend Micro minimizes complexity by giving you a unified view of security insights, enabling you to make data-driven security decisions. Trend Micro Cloud One – Open Source Security by Snyk provides rich contextual information about security vulnerabilities found in open source dependencies. This enables developer and security operations teams to gain deeper visibility into their code and to prioritize issues.


TREND MICRO
Trend Micro Cloud One™: Cloud Security Services Platform
Access via Trend Micro Cloud One
snyk
✓ Integrate with third-party source code repositories and CI/CD tools e.g., GitLab, GitHub, Jenkins
One Group
One Organization
✓ Aggregate data at the group and org level
✓ Vulnerability and license reporting
Projects
✓ Tag projects
✓ Scan for open source vulnerabilities
✓ Apply open source license policy

››› Back to TOP

Using the Snyk vulnerability database



package.json

Created Fri 26th Mar 2021 | Snapshot taken by recurring test 18 hours ago

IMPORTED BY: 185670003643e5dc@cloudone.trendmicro.com

PROJECT OWNER: Add a project owner

TESTED WITH: package-lock.json,package.json

ENVIRONMENT: Add a value

BUSINESS CRITICALITY: Add a value

LIFECYCLE STAGE: Add a value

TAGS: Add a key/value…

```
goof@1.0.1
├─ H adm-zip@0.4.7
├─ body-parser@1.9.0                 -
│  └─ H qs@2.2.4
├─ cfenv@1.2.2                       -
│  └─ L underscore@1.9.1
├─ H dustjs-linkedin@2.5.0
├─ H M ejs@1.0.0
├─ ejs-locals@1.0.2                  -
│  └─ H M ejs@0.8.8
├─ errorhandler@1.2.0                +
└─ express@4.12.4                    +
```

- **Dependency tree view.** Accelerate the triaging process with a dependency path analysis. Understand the path through which transitive vulnerabilities have been introduced.
- **Dependency health.** Broaden your security coverage by identifying risks associated with dependencies inside your open source libraries.
- **Runtime prioritization.** Prioritize your fixes based on an analysis of the vulnerabilities called at runtime and that bear a higher risk.
- **Exploit maturity.** Use indicators to identify exploits that attackers can easily weaponize.
- **Accuracy control.** Receive high-accuracy alerts that are verified and qualified by Snyk's dedicated security research team.

››› Back to TOP

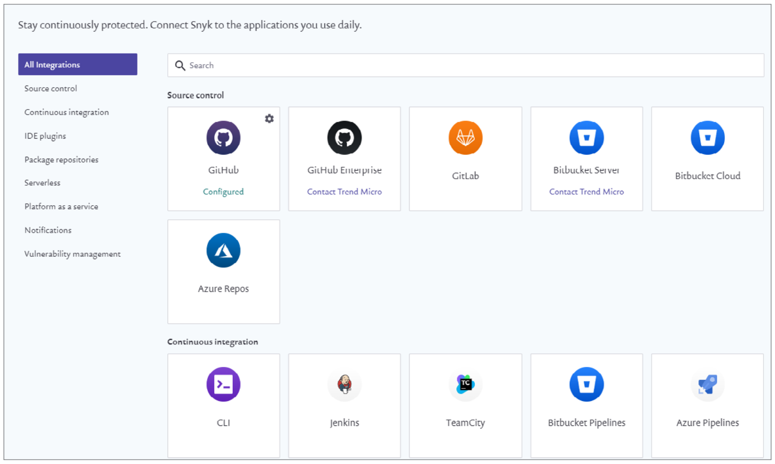
How to Get Started

Trend Micro Cloud One – Open Source Security by Snyk “integration” is a pre-existing implementation that can connect to various tools based on your configuration (like source control or container registries) to discover your application. To set up an integration, administrators configure one or more of the tiles in the UI “integrations” tab. Configuration occurs on each tile and requires credentials or an API key. Each integration can contain additional configuration settings specific to the integration.

After setup, each integration will provide users the ability to import projects. (See below for import instructions)

Trend Micro Cloud One – Open Source Security by Snyk supports integration with Git-based solutions like GitHub, and GitLab, as well as integrations such as Azure Repos, Jenkins, AWS Lambda, Artifactory, Bitbucket, GoLand, and more.

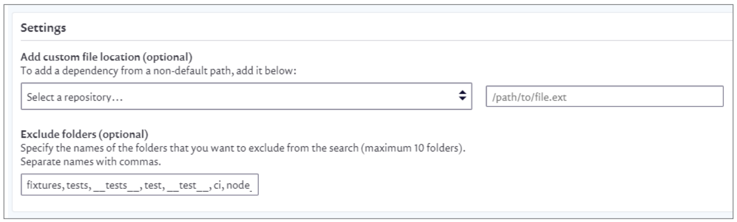
In Trend Micro Cloud One – Open Source Security by Snyk, information is organized based on projects. A project represents a list of issues which includes both vulnerabilities and license compliance issues. Issues are determined by analyzing the package manager of your application and reviewing the direct and indirect dependencies. When developers create an application, they list the direct dependencies needed, which have their own dependencies called “indirect dependencies”. (See direct and indirect dependencies in the “Dependency Tree View” section).



Stay continuously protected. Connect Snyk to the applications you use daily.

››› Back to TOP

Importing projects can be completed using various methods. The two most common are Trend Micro Cloud One – Open Source Security by Snyk UI or the CLI. Use the Trend Micro Cloud One – Open Source Security by Snyk UI to import projects by selecting the integration from the list. (See below for an example using GitHub).



Settings

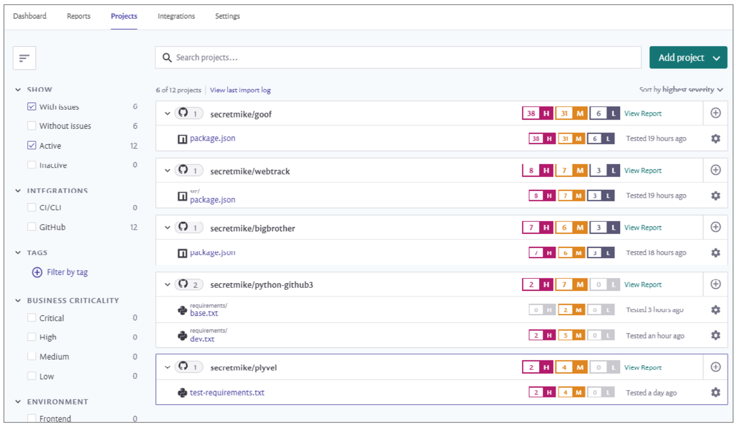
Add custom file location (optional)
To add a dependency from a non-default path, add it below:

Select a repository… | /path/to/file.ext

Exclude folders (optional)
Specify the names of the folders that you want to exclude from the search (maximum 10 folders).
Separate names with commas.

fixtures, tests, __tests__, test, __test__, ci, node_

When the import is complete, the Trend Micro Cloud One- Open Source Security by Snyk console will list the package and number of issues detected. Opening the display highlights vulnerabilities, severity level, and exploit maturity. Drill down further into the dependency tree.



SHOW
- ☑ With issues 6
- □ Without issues 6
- ☑ Active 12
- □ Inactive 0

INTEGRATIONS
- □ CI/CLI 0
- □ GitHub 12

TAGS
- Filter by tag

BUSINESS CRITICALITY
- □ Critical 0
- □ High 0
- □ Medium 0
- □ Low 0

ENVIRONMENT
- □ Frontend 0

6 of 12 projects | View last import log — Sort by highest severity

Project	H	M	L	
secretmike/goof (1)	38	31	6	View Report
package.json	38	31	6	Tested 19 hours ago
secretmike/webtrack (1)	8	7	3	View Report
src/ package.json	8	7	3	Tested 19 hours ago
secretmike/bigbrother (1)	7	6	3	View Report
package.json	7	6	3	Tested 18 hours ago
secretmike/python-github3 (2)	2	7	0	View Report
requirements/ base.txt	0	2	0	Tested 3 hours ago
requirements/ dev.txt	2	5	0	Tested an hour ago
secretmike/plyvel (1)	2	4	0	View Report
test-requirements.txt	2	4	0	Tested a day ago

To learn more about how to deploy or analyze Trend Micro Cloud One – Open Source Security by Snyk visit the Trend Micro Cloud One Documentation.

››› Back to TOP

Considerations

Trend Micro Cloud One – Open Source Security by Snyk is powered by the leading vulnerability database, providing comprehensive and actionable open source vulnerability intelligence.

- **Dedicated team of security experts.** The Snyk Vulnerability Database is managed by experts, researchers, and analysts. This team ensuring the database maintains a high level of accuracy with a low false-positive rate.

- **Curated, enriched, and actionable content.** The team enriches the data describing each vulnerability with hand-curated content and summaries, including code snippets where applicable. All items in the database are analyzed and tested for their accuracy (for example; version ranges, vulnerable method). A CVSS score and vector is assigned to 100% of vulnerabilities.

- **Beyond CVE/NVD.** The Snyk Vulnerability Database expands far beyond CVE vulnerabilities and includes many additional non-CVE vulnerabilities that are derived from additional sources.

- **Best coverage in the market.** Snyk has regularly outperformed other vendors in head-to-head evaluations against other vulnerability identification vendors.

- **First to know and publish.** Snyk exposes many vulnerabilities before they are added to public databases. On average:

    - Snyk publishes vulnerabilities 92 days sooner than NPM Audit
    - Discovers 370% more vulnerabilities
    - Identifies vulnerabilities 25 days faster
    - 92% of the JavaScript vulnerabilities in NVD were added first to the Snyk database

››› Back to TOP

Why Trend Micro Cloud One – Open Source Security by Snyk

As part of the Trend Micro Cloud One™ SaaS security platform, Trend Micro Cloud One – Open Source Security by Snyk provides visibility and tracking of vulnerabilities and license issues of open source dependencies. With this advanced service, Security Operations teams are able to gain awareness of open source vulnerabilities and license risks in their applications for better risk management.

Trend Micro Cloud One gives you complete security and insight into the protection of your applications. Your team is provided with a view into the prioritizations of the risks and threats that can impact your runtime security. Trend Micro Cloud One – Open Source Security by Snyk enables you to dive deeper into your application security threats with visibility into the dependency paths and transitive vulnerabilities.

Trend Micro provides security teams with visibility sooner in their build cycles to reduce threats earlier. Security teams are connected with development teams to create a common tool that can drive risk management and help mitigate open source security bugs within your application code base.

TREND MICRO™

Securing Your
Connected World

[UGOO_Cloud_One_Open_Source_User_Guide_210511US]

››› Back to TOP