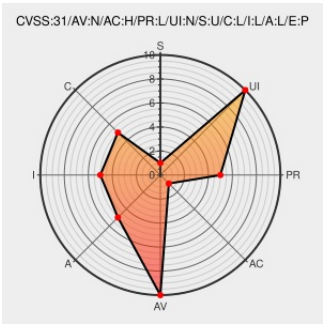
CVE-2022-22984

Published on: Not Yet Published

Last Modified on: 12/02/2022 06:59:00 PM UTC

CVE-2022-22984

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Snyk Cli from Snyk contain the following vulnerability:

The package snyk before 1.1064.0; the package snyk-mvn-plugin before 2.31.3; the package snyk-gradle-plugin before 3.24.5; the package @snyk/snyk-cocoapods-plugin before 2.5.3; the package snyk-sbt-plugin before 2.16.2; the package snyk-python-plugin before 1.24.2; the package snyk-docker-plugin before 5.6.5; the package @snyk/snyk-hex-plugin before 1.1.6 are vulnerable to Command Injection due to an incomplete fix for [CVE-2022-40764](https://security.snyk.io/vuln/SNYK-JS-SNYK-3037342). A successful exploit allows attackers to run arbitrary commands on the host system where the Snyk CLI is installed by passing in crafted command line flags. In order to exploit this vulnerability, a user would have to execute the snyk test command on untrusted files. In most cases, an attacker positioned to control the command line arguments to the Snyk CLI would already be positioned to execute arbitrary commands. However, this could be abused in specific scenarios, such as continuous integration pipelines, where developers can control the arguments passed to the Snyk CLI to leverage this component as part of a wider attack against an integration/build pipeline. This issue has been addressed in the latest Snyk Docker images available at https://hub.docker.com/r/snyk/snyk as of 2022-11-29. Images downloaded and built prior to that date should be updated. The issue has also been addressed in the Snyk TeamCity CI/CD plugin as of version v20221130.093605.

CVE-2022-22984 has been assigned by report@snyk.io to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	LOW	LOW

CVE References

Description	Tags	Link
Command Injection in @snyk/snyk-cocoapods-plugin | CVE-2022-22984 | Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-JS-SNYKSNYKCOCOAPODSPLUGIN-3038625
fix: quote spawn args · snyk/snyk-hex-plugin@e8dd2a3 · GitHub	github.com text/html	MISC github.com/snyk/snyk-hex-plugin/commit/e8dd2a330b40d7fc0ab47e34413e80a0146d7ac3
How Scanning Your Projects for Security Issues Can Lead to Remote Code Execution | Imperva	www.imperva.com text/html	MISC www.imperva.com/blog/how-scanning-your-projects-for-security-issues-can-lead-to-remote-code-execution/
fix: quote spawn args · snyk/snyk-python-plugin@8591abd · GitHub	github.com text/html	MISC github.com/snyk/snyk-python-plugin/commit/8591abdd9236108ac3e30c70c09238d6bb6aabf4
fix: escape child process arguments · snyk/cli@80d97a9 · GitHub	github.com text/html	MISC github.com/snyk/cli/commit/80d97a93326406e09776156daf72e3caa03ae25a
fix: quote spawn args · snyk/snyk-docker-plugin@d730d76 · GitHub	github.com text/html	MISC github.com/snyk/snyk-docker-plugin/commit/d730d7630691a61587b120bb11daaaf4b58a8357
Command Injection in snyk-python-plugin | CVE-2022-22984 | Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-JS-SNYKPYTHONPLUGIN-3039677
Command Injection in snyk | CVE-2022-22984 | Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-JS-SNYK-3038622
fix: escape child process arguments · snyk/snyk-mvn-plugin@02cda9b · GitHub	github.com text/html	MISC github.com/snyk/snyk-mvn-plugin/commit/02cda9ba1ea36b00ead3f6ec2de0f97397ebec50
fix: quote args · snyk/snyk-cocoapods-plugin@c73e049 · GitHub	github.com text/html	MISC github.com/snyk/snyk-cocoapods-plugin/commit/c73e049c5200772babde61c40aab57296bf91381
Command Injection in @snyk/snyk-hex-plugin | CVE-2022-22984 | Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-JS-SNYKSNYKHEXPLUGIN-3039680
fix: escape child process arguments · snyk/snyk-gradle-plugin@bb1c1c7 · GitHub	github.com text/html	MISC github.com/snyk/snyk-gradle-plugin/commit/bb1c1c72a75e97723a76b14d2d73f70744ed5009
Command Injection in snyk-mvn-plugin | CVE-2022-22984 | Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-JS-SNYKMVNPLUGIN-3038623
fix: escape child process arguments · snyk/snyk-sbt-plugin@99c09eb · GitHub	github.com text/html	MISC github.com/snyk/snyk-sbt-plugin/commit/99c09eb12c9f8f2b237aea9627aab1ae3cab6437
Command Injection in snyk-docker-plugin | CVE-2022-22984 | Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-JS-SNYKDOCKERPLUGIN-3039679
Command Injection in snyk-gradle-plugin | CVE-2022-22984 | Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-JS-SNYKGRADLEPLUGIN-3038624
Command Injection in snyk-sbt-plugin | CVE-2022-22984 | Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-JS-SNYKSBTPLUGIN-3038626

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Snyk	Snyk Cli	All	All	All	All
Application	Snyk	Snyk Cocoapods Cli	All	All	All	All
Application	Snyk	Snyk Docker Cli	All	All	All	All
Application	Snyk	Snyk Gradle Cli	All	All	All	All
Application	Snyk	Snyk Hex Cli	All	All	All	All
Application	Snyk	Snyk Maven Cli	All	All	All	All
Application	Snyk	Snyk Python Cli	All	All	All	All
Application	Snyk	Snyk Sbt Cli	All	All	All	All

cpe:2.3:a:snyk:snyk_cli:*:*:*:*:*:*:*:*:

cpe:2.3:a:snyk:snyk_cocoapods_cli:*:*:*:*:*:snyk:*:*:

cpe:2.3:a:snyk:snyk_docker_cli:*:*:*:*:*:snyk:*:*:

cpe:2.3:a:snyk:snyk_gradle_cli:*:*:*:*:*:snyk:*:*:

cpe:2.3:a:snyk:snyk_hex_cli:*:*:*:*:*:snyk:*:*:

cpe:2.3:a:snyk:snyk_maven_cli:*:*:*:*:*:snyk:*:*:

cpe:2.3:a:snyk:snyk_python_cli:*:*:*:*:*:snyk:*:*:

cpe:2.3:a:snyk:snyk_sbt_cli:*:*:*:*:*:snyk:*:*:

Discovery Credit

Ron Masas - Imperva

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-22984 : The package snyk before 1.1064.0; the package snyk-mvn-plugin before 2.31.3; the package snyk-grad… twitter.com/i/web/status/1…	2022-11-30 12:54:25
@JohnJasonFallow	New vulnerability on the NVD: CVE-2022-22984 ift.tt/4ksJ6PT	2022-11-30 15:13:33
@doogsineerg	New vulnerability on the NVD: CVE-2022-22984 ift.tt/GrSPEWQ	2022-11-30 15:48:03
@4ng3n01r3	#CyberSecurity #Security #CERT #CVE #Nist #breach #vulnerability : CVE-2022-22984	2022-11-30 15:55:19
@workentin	New vulnerability on the NVD: CVE-2022-22984 ift.tt/pJhLMcs	2022-11-30 15:55:23
@xanadulinux	CVE-2022-22984 ift.tt/mnOY3Lk	2022-11-30

		16:11:44
/r/netcve	CVE-2022-22984	2022-11-30 13:45:55

← Previous ID

Next ID→