Code Injection

Affecting snyk package, versions <1.1064.0

INTRODUCED: 29 SEP 2022 CVE-2022-24441 ? CWE-77 ? FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `snyk` to version 1.1064.0 or higher.

Overview

snyk is a advanced tool that scans and monitors projects for security vulnerabilities.

Affected versions of this package are vulnerable to Code Injection. when analyzing a project. An attacker who can convince a user to scan a malicious project can include commands in a build file such as `build.gradle` or `gradle-wrapper.jar`, which will be executed with the privileges of the application.

This vulnerability may be triggered when running the the CLI tool directly, or when running a scan with one of the IDE plugins that invoke the Snyk CLI.

Successful exploitation of this issue would likely require some level of social engineering - to coerce an untrusted project to be downloaded and analyzed via the Snyk CLI or opened in an IDE where a Snyk IDE plugin is installed and enabled. Additionally, if the IDE has a Trust feature then the target folder must be marked as 'trusted' in order to be vulnerable.

NOTE: This issue is independent of the one reported in CVE-2022-40764, and upgrading to a fixed version for this addresses that issue as well.

The affected IDE plugins and versions are:

- VS Code - Affected: <=1.8.0, Fixed: 1.9.0
- IntelliJ - Affected: <=2.4.47, Fixed: 2.4.48
- Visual Studio - Affected: <=1.1.30, Fixed: 1.1.31
- Eclipse - Affected: <=v20221115, Fixed: v20221130
- Language Server - Affected: <=v20221109, Fixed: v20221130

References

- GitHub Commit (snyk-eclipse-plugin)
- GitHub Commit (snyk-intellij-plugin)
- GitHub Commit (snyk-ls)
- GitHub Commit (snyk-visual-studio-plugin)
- GitHub Commit (vscode-extension)
- Imperva Blog Post
- Snyk Blog Post

5.8

MEDIUM

Snyk CVSS

Attack Complexity	High ?
User Interaction	Required ?
Scope	Changed ?

See more

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-JS-SNYK-3111871
Published	30 Nov 2022
Disclosed	29 Sep 2022
Credit	Ron Masas - Imperva

Report a new vulnerability

Found a mistake?

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.