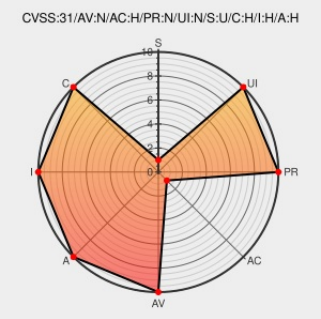
CVE-2022-24440

Published on: Not Yet Published

Last Modified on: 04/08/2022 07:08:00 PM UTC

CVE-2022-24440

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



Certain versions of Cocoapods-downloader from Cocoapods contain the following vulnerability:

The package cocoapods-downloader before 1.6.0, from 1.6.2 and before 1.6.3 are vulnerable to Command Injection via git argument injection. When calling the Pod::Downloader.preprocess_options function and using git, both the git and branch parameters are passed to the git ls-remote subcommand in a way that additional flags can be set. The additional flags can be used to perform a command injection.

CVE-2022-24440 has been assigned by report@snyk.io to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Ensure that the git pre-processor doesn't accidentally bail also by orta · Pull Request #128 · CocoaPods/cocoapods-downloader · GitHub	github.com text/html	MISC github.com/CocoaPods/cocoapods-

		downloader/pull/128
Adds a check for command injections in the input for hg and git by orta · Pull Request #124 · CocoaPods/cocoapods-downloader · GitHub	github.com text/html	MISC github.com/CocoaPods/cocoapods-downloader/pull/124
Command Injection in cocoapods-downloader | CVE-2022-24440 | Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-RUBY-COCOAPODSDOWNLOADER-2414278

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cocoapods	Cocoapods-downloader	All	All	All	All
Application	Cocoapods	Cocoapods-downloader	1.6.2	All	All	All

cpe:2.3:a:cocoapods:cocoapods-downloader:*:*:*:*:*:*:*:*:

cpe:2.3:a:cocoapods:cocoapods-downloader:1.6.2:*:*:*:*:*:*:*:

Discovery Credit

Alessio Della Libera of Snyk Research Team

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-24440 : The package cocoapods-downloader before 1.6.0, from 1.6.2 and before 1.6.3 are vulnerable to Comma… twitter.com/i/web/status/1…	2022-04-01 17:37:11
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-24440 The package cocoapods-downloader before 1.6.0, from 1.6.2 and bef… twitter.com/i/web/status/1…	2022-04-01 18:56:01
/r/netcve	CVE-2022-24440	2022-04-01 18:38:38

← Previous ID

Next ID→