Remote code execution in dependabot-core branch names when cloning

Low feelepxyz published GHSA-23f7-99jx-m54r on Nov 13, 2020

Package

dependabot-omnibus,dependabot-common,dependabot-go_modules (bundler)

Affected versions	Patched versions
>= v0.119.0.beta1, < 0.125.1	0.125.1

Description

Impact

Remote code execution vulnerability in `dependabot-common` and `dependabot-go_modules` when a source branch name contains malicious injectable bash code.

For example, if Dependabot is configured to use the following source branch name: `"/$({curl,127.0.0.1})"`, Dependabot will make a HTTP request to the following URL: 127.0.0.1 when cloning the source repository.

When Dependabot is configured to clone the source repository during an update, Dependabot runs a shell command to git clone the repository:

```
git clone --no-tags --no-recurse-submodules --depth=1 --branch=<BRANCH> --single-branch <GITHUB_REPO_URL> repo/contents/path
```

Dependabot will always clone the source repository for `go_modules` during the file fetching step and can be configured to clone the repository for other package managers using the `FileFetcher` class from `dependabot-common`.

```
source = Dependabot::Source.new(
  provider: "github",
  repo: "repo/name",
  directory: "/",
  branch: "/$({curl,127.0.0.1})",
)

repo_contents_path = "./file/path"
fetcher = Dependabot::FileFetchers.for_package_manager("bundler").
                  new(source: source, credentials: [],
                  repo_contents_path: repo_contents_path)
fetcher.clone_repo_contents
```

Patches

The fix was applied to version `0.125.1`: #2727

Workarounds

Escape the branch name prior to passing it to the `Dependabot::Source` class.

For example using `shellwords`:

```
require "shellwords"
branch = Shellwords.escape("/$({curl,127.0.0.1})")
source = Dependabot::Source.new(
  provider: "github",
  repo: "repo/name",
  directory: "/",
  branch: branch,
)
```

Severity

Low

CVE ID

CVE-2020-26222

Weaknesses

No CWEs

Credits

mrthankyou