bitnami / bitnami-docker-laravel Public archive

Code Issues Pull requests Actions Projects Security Insights

Laravel APP_KEY is fixed in docker image bitnami/laravel #139

Closed **beltran-rubo** opened this issue on Mar 2, 2021 · 2 comments

Assignees

beltran-rubo commented on Mar 2, 2021 • edited

Description

The file /tmp/app/.env is generated at the time that the docker image bitnami/laravel was built, and the value of APP_KEY is fixed under certain conditions. Although the APP_KEY will generated randomly each time we install laravel:

```
"@php artisan key:generate --ansi"
```

But if we build it as a docker image, the APP_KEY is a fixed value whenever we run it. This value is crucial for the security of the application and must be randomly generated per Laravel installation.

An attacker would be able to perform a deserialization attack, for instance using a Laravel vulnerability CVE-2018-15133. If your application's encryption key is in the hands of a malicious party, that party could craft cookie values using the encryption key and exploit vulnerabilities inherent to PHP object serialization / unserialization, such as calling arbitrary class methods within your application.

Fix

The Entrypoint now regenerates the APP_KEY if the app is not mounted and copied from the default one. This issue was reported by LEI WANG on February the 23rd and it was fixed on Feburary the 24th. The following container images have been released with the fix:

- 6.20.0-debian-10-r107 or newer
- 7.30.1-debian-10-r108 or newer
- 8.5.11-debian-10-r0 or newer

UPDATED: The CVE assigned for this issue is CVE-2021-21979.

Mauraza pinned this issue on Mar 3, 2021

beltran-rubo added the **on-hold** label on Mar 3, 2021

beltran-rubo self-assigned this on Mar 3, 2021

ZsgsDesign commented on Sep 11, 2021 • edited

If maintainers really want to fix the value of APP_KEY in production environment, isn't that better to add a `APP_KEY` environment variable via env option or through `docker-compose.yml` when started the container? I believe it is not a bug but how maintainers should maintain their docker container.

beltran-rubo commented on Sep 13, 2021 Author

Hi **@ZsgsDesign**, yes that could be an option. In this case it will be generated **only** if the app folder does not exist, only when the sample laravel app is generated.

bitnami-docker-laravel/8/debian-10/rootfs/app-entrypoint.sh
Line 90 in `e86fa12`

```
90      if [[ ! -d /app/app ]]; then
```

🎉 2

beltran-rubo closed this as completed on Sep 13, 2021

carrodher removed the **on-hold** label on Dec 26, 2021

Assignees

beltran-rubo

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants