CVE-2020-13794 Harbor User Enumeration Vulnerability

Wednesday, Sep 16, 2020

Harbor

During a recent pentest engagement, one of my targets was Harbor. The version tested was 1.9.3 however, this vulnerability most likely works on earlier versions as well.

A non-administrator account was provided during the pentest engagement.

> Harbor is an open source trusted cloud native registry project that stores, signs, and scans content. Harbor extends the open source Docker Distribution by adding the functionalities usually required by users such as security, identity and management. Having a registry closer to the build and run environment can improve the image transfer efficiency. Harbor supports replication of images between registries, and also offers advanced security features such as user management, access control and activity auditing.[1]

Security Advisories

While analyzing the target I decided to look up security advisories posted on github. Even though the security advisories contain patched vulnerabilities, they can provide insight and inspiration for potential undiscovered vulnerabilities.

One security advisory which caught my eye is an user enumeration vulnerability. It is a pretty straight forward vulnerability where you send a request to the search API endpoint containing an e-mail or part of it and in return, you receive a response containing user information.

An example given in the security advisory:

```
curl -X GET "http://<host>/api/users/search?email=test@test.com" -H "accept: application/json" --user <user>:<password>
```

Finding a new vulnerability

Having the user enumeration vulnerability security advisory in mind. I decided to try and find other query strings that might result in a similar vulnerability. This can easily be tested using Burp Suite's intruder or just any tool would do.

One query string which seemed to work is username. It is possible to list all users containing a given letter using the following cURL command:

```
curl -X GET "http://<host>/api/users/search?username=X" -H "accept: application/json" --user <user>:<password>
```

My next attempt was to find a wildcard character to display all users available. After running every single character through the cURL request the following cURL request seemed to display all users currently registered:

```
curl -X GET "http://<host>/api/users/search?username=_" -H "accept: application/json" --user <user>:<password>
```

As shown in the example above, the underscore character acts as a wildcard character.

The information given by this API is an `user_id` and `username`. During the pentest engagement, most of the usernames discovered contained e-mail addresses. Providing a nice list of targets for social engineering attacks.

After discovering this vulnerability I informed Harbor Security Team, they confirmed the vulnerability which has been assigned to CVE-2020-13794.

Remediation

The Harbor Security Team has published a security advisory regarding this vulnerability (GHSA-g9p8-33wc-h432).

This issue is resolved in version 2.1.0 and 2.0.3.

---

1. https://github.com/goharbor/harbor ↩