Authenticated users can exploit an enumeration vulnerability in Harbor (CVE-2020-13794)

Low **michmike** published **GHSA-q9p8-33wc-h432** on Sep 28, 2020

Package

Harbor

Affected versions	Patched versions
1.9.*, 1.10.*, 2.0.*	2.0.3, 2.1.0

Description

Impact

Hidde Smit from Cyber Eagle has discovered an User Enumeration flaw in Harbor. The issue is present in the "/users" api endpoint. This endpoint is supposed to be restricted to administrators. This restriction is able to be bypassed and information can be obtained via the "search" functionality.

Non-administrator users (such as those created via self-registration) can list all usernames and user IDs by sending a GET request to /api/users/search with parameter "username" and value "_", as follows:

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

The vulnerability was immediately fixed by the Harbor team and all supported versions were patched. With the patched versions of Harbor, the username is required for search and we have removed the support for querying by email.

Patches

If your product uses the affected releases of Harbor, update to either version 2.1.0 or 2.0.3 to fix this issue immediately

https://github.com/goharbor/harbor/releases/tag/v2.1.0
https://github.com/goharbor/harbor/releases/tag/v2.0.3

Workarounds

There is no workaround for this issue

For more information

If you have any questions or comments about this advisory, contact cncf-harbor-security@lists.cncf.io
View our security policy at https://github.com/goharbor/harbor/security/policy
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13794

Severity

Low

CVE ID

CVE-2020-13794

Weaknesses

No CWEs