huntr

# SQL injetction in camptocamp/terraboard

1

✓ Valid Reported on May 19th 2022

## Description

SQL injection exists in the camptocamp/terraboard.
Among all APIs there is an API routed to `/api/search/attribute`, whose corresponding method is api.SearchAttribute. In the api.SearchAttribute method, the program takes the request parameters and passes them into the db.SearchAttribute method. In the db.SearchAttribute method, when the request parameter `tf_version` or `lineage_value` is set, the program executes up to line 373 or 377. In these two lines, the program is dynamically splicing strings, which may lead to SQL injection.
As an example, part of the code on line 373 is as follows.

```
fmt.Sprintf("states.tf_version LIKE '%s'", fmt.Sprintf("%%%s%%", v))
```

where the variable `v` is the request parameter `tf_version`, which is user controllable. When the variable `v` is the following string.

```
v := "' OR pg_sleep(10) OR states.tf_version LIKE '%"
```

The sql statement will then change to `"states.tf_version LIKE '%' OR pg_sleep(10) OR states.tf_version LIKE '%%'"`, This will cause pgsql to execute the `pg_sleep` function. Replacing `pg_sleep` with another statement will lead to more serious consequences.

## Proof of Concept

Try executing the following `curl` command which should have the effect of the request taking 10 seconds to get a response. Where `$DEMO_URL` is the address and port of the APP.

```
curl "http://${DEMO_URL}/api/search/attribute?tf_version='+OR
```

## Impact

sql injection can lead to sensitive data leakage and even the acquisition of server privileges.

## Occurrences

db.go L373 db.go L377

## References

- https://portswigger.net/web-security/sql-injection

CVE
CVE-2022-1883
(Published)

Vulnerability Type
CWE-89: SQL Injection

Severity
Critical (9.6)

Registry
Golang

Affected Version
<=v2.1.1

Visibility
Public

Status
Fixed

Found by

AFKL
@afkl-cuit
unranked

This report was seen 972 times.

We are processing your report and will contact the **camptocamp/terraboard** team within 24 hours. 6 months ago

**AFKL** modified the report 6 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 6 months ago

We have contacted a member of the **camptocamp/terraboard** team and are waiting to hear back 6 months ago

A **camptocamp/terraboard** maintainer 6 months ago

Maintainer

Hello AFKL and thanks for the detailed report,

FYI , you can easily build a working teraboard with postgres and everything using the docker-compose.yaml available at the root of the repository.

We could not trigger the bug, here is what we did using the docker-compose

```
time curl "http://127.0.0.1:8080/api/search/attribute?tf_version='+OR+pg_sleep(10)+OR+
{"page":1,"results":[],"total":0}
curl  0.00s user 0.00s system 42% cpu 0.019 total
```

Regards

Julien@c2c

AFKL 6 months ago

Researcher

Hello!
Thank you, I thought an AWS account was a must and I have successfully set up a test environment.

I am sorry that the previous exp was wrong. After testing, the following exp is valid.

```
PS C:\Users\AFKL> time curl "http://127.0.0.1:8080/api/search/attrit
{"page":1,"results":null,"total":0}real 0m 10.06s
user    0m 0.01s
```

Chat with us

```
sys     0m 0.00s
```

A camptocamp/terraboard maintainer 6 months ago Maintainer

Hello,
We reproduced the bug.
The patch is on its way, we are waiting for the new release to "valid and Fixed".
Thanks for the report AFKL.
Regards
J\x00

AFKL 6 months ago Researcher

Thank you for your fix 👍, I will amend the title and preface section of the report.

One other thing, can we assign a CVE to this vulnerability? This will help users to get timely notification of vulnerability fixes. :D @admin

AFKL modified the report 6 months ago

A camptocamp/terraboard maintainer 6 months ago Maintainer

Yes, you can ask for a CVE (I think it as already been asked ? )
I am filling up the report form.
Regards
J\x00

A camptocamp/terraboard maintainer validated this vulnerability 6 months ago

AFKL has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

A camptocamp/terraboard maintainer marked this as fixed in 2.2.0 with c
6 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

**db.go#L373** has been validated ✓

**db.go#L377** has been validated ✓

Sign in to join this conversation