New issue

Jump to bottom

Security flaw in default configuration of webui #764

Open **martinzhou2015** opened this issue on Jan 15, 2021 · 9 comments

martinzhou2015 commented on Jan 15, 2021 • edited

Details

The configuration of `webui` might result in the control panel being taken over by arbitrary user via default username and password.

The lines of code below indicate that, if not specified, the server will listen on `0.0.0.0:3000`, which means the control panel could be accessed via WAN.

```
https://github.com/open5gs/open5gs/blob/master/webui/server/index.js#L3
const _hostname = process.env.HOSTNAME || '0.0.0.0';
const port = process.env.PORT || 3000;
```

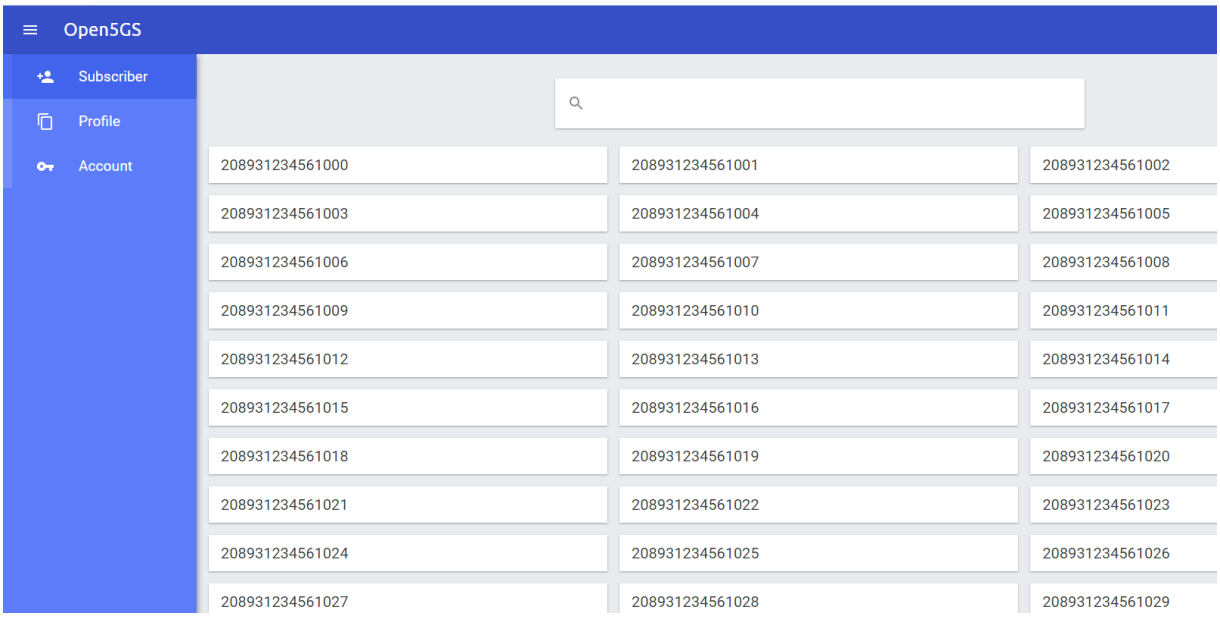
On `Line 38`, the code will create a default account `admin / 1423`, if there isn't any account specified in MongoDB.

```
const db = yield mongoose.connect(process.env.DB_URI, {
    useMongoClient: true,
    /* other options */
  })

  Account.count((err, count) => {
    if (err) {
      console.error(err);
      throw err;
    }

    if (!count) {
      const newAccount = new Account();
      newAccount.username = 'admin';
      newAccount.roles = [ 'admin' ];
      Account.register(newAccount, '1423', err => {
        if (err) {
          console.error(err);
          throw err;
        }
      })
    }
```

Proof of Concept

After doing a query via Zoomeye, a search engine that lets the user find specific types of computers connected to the internet using a variety of filters, several vulnerable cases have been found:

```
http://140.118.155.145:3000/
http://194.135.39.106:3000/

* Source: https://www.zoomeye.org/searchResult?q=title%3A%22Open5GS%22%20%2Bafter:%222021-01-01%22%20%2Bbefore:%222022-01-01%22&t=all
```



Suggestion

The default account should never be assigned automatically.

acetcom commented on Jan 18, 2021 — Member

@martinzhou2015 Is there a good way to get started with open5gs without adding a default user?

nickvsnetworking commented on Jan 21, 2021 — Contributor

@acetcom A few options:

Could we add a config file for the WebUI to allow access only to predefined subnets? We could add the local subnet to the config file during the install, and if a user wanted to open it up to more subnets they could change the config file themselves?

- Force a password change on first login (Easy)
- Randomly generate a password during the install (Annoying for the user to get the output)
- Restrict access to only local subnets by default and add a config file to change this behaviour (some work to implement)

I could potentially add the forced password change on first login functionality if you think that's the best path?

kbarlee commented on Jan 21, 2021 — Sponsor, Contributor

The bind on 0.0.0.0 is a consequence of #587

acetcom commented on Jan 22, 2021 — Member

Hi, all

Here is my idea.

Running with `npm run dev` uses the same method as it is now. In development mode, I think it's okay to do it like now.

However, installing in production mode will not use the current code. The admin user will be added automatically during the installation phase.

```
#  The admin user is automatically added in the following script.
$ curl -sL https://open5gs.org/open5gs/assets/webui/uninstall | sudo -E bash -
```

Let me know if you have different idea.

Thanks a lot!
Sukchan

cecrevier commented on Jan 23, 2021

i think personally its already fine like it was.
EPC should never be installed directly on Internet but behind firewall on natted network.
Management network should be different as UE network also.
its like anythings, when you install something on the public network you need to think and secure it properly.

martinzhou2015 commented on Jan 26, 2021 — Author

> Hi, all
>
> Here is my idea.
>
> Running with `npm run dev` uses the same method as it is now. In development mode, I think it's okay to do it like now.
>
> However, installing in production mode will not use the current code. The admin user will be added automatically during the installation phase.
>
> ```
> #  The admin user is automatically added in the following script.
> $ curl -sL https://open5gs.org/open5gs/assets/webui/uninstall | sudo -E bash -
> ```
>
> Let me know if you have different idea.
>
> Thanks a lot!
> Sukchan

I think it's better to:
`Force a password change on first login` OR `Let the user to specify a password on their own when setting up`

To secure a system, under no circumstance, a default weak password should be assigned automatically.

OS-WS commented on Apr 26, 2021

Hi, this issue was assigned with CVE-2021-25863.
is there a fix for it?

acetcom commented on Apr 28, 2021 — Member

@OS-WS

I forgot this problem. I'll get back to you here when it's modified.

Thank you for reminding me.
Sukchan

acetcom added a commit that referenced this issue on May 8, 2021

`[WebUI] fix the security flaw in account (#764)` ··· ✓ `26f14ee`

acetcom commented on May 8, 2021 — Member

@OS-WS

I've fixed this issues as described below.

- In developement mode, if there is no default admin account, the Node.js server WILL create admin/1423 account.
- In production mode, even though there is no default admin account, the Node.js server WILL NOT create admin/1423 account.

I've also improved the WebUI installation script as follows:

1. WebUI installation script creates a default admin account if there is no account.

```
### WebUI installation script
$ curl -fsSL https://open5gs.org/open5gs/assets/webui/install | sudo -E bash -
```

2. If WebUI is already installed, the installation script automatically uninstalls WebUI first and then starts the installation.

It will be applied to the v2.2.8 package in the near future.

Let me know if you have any further questions.

Thanks a lot!
Sukchan

acetcom mentioned this issue on May 8, 2021

failure to install and activate open5gs webUI according to QuickInstall #971

Closed

acetcom added a commit that referenced this issue on Oct 23, 2021

`WebUI uses localhost by default (#764, #587)` ✓ `608c083`

WR1171 mentioned this issue on Nov 1

WebUI error in MongoDB 6.0 #1824

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

6 participants