New issue

Jump to bottom

Authentication Bypass in Webui #837

Open rashley-iqt opened this issue on Mar 10, 2021 · 0 comments

rashley-iqt commented on Mar 10, 2021 Contributor

An unauthenticated user can utilize information provided by the login page of the webui component to craft HTTP requests that will allow that user to create, read, update, and delete entries in the subscriber database. This includes the ability to add administrative users, add/modify/delete subscribers, and add/modify/delete profiles.

Properly crafted HTTP GET and DELETE requests with empty bodies will cause data to be returned or deleted on the following routes:
http://:3000/api/db/account
http://:3000/api/db/profile
http://:3000/api/db/subscriber
http://:3000/api/db/account/
http://:3000/api/db/profile/<profile_id>
http://:3000/api/db/subscriber/<imsi_number>

Properly crafted HTTP POST,PUT and PATCH requests with properly crafted bodies will cause data to be inserted or updated on the following routes:
http://:3000/api/db/account
http://:3000/api/db/profile
http://:3000/api/db/subscriber
http://:3000/api/db/account/
http://:3000/api/db/profile/<profile_id>
http://:3000/api/db/subscriber/<imsi_number>

This is caused by the configuration of express js in index.js. This should be updated to correctly validate the user making the API calls.

This was referenced on Mar 10, 2021

Add API tokens #838

Merged

Authentication Bypass in Webui nextepc/nextepc#31

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant