andrey-lomtev / **CVE-2021-37934**

Last active last year

☆ Star

Code Revisions 2

CVE-2021-37934

```
CVE-2021-37934
------------------------------------------
Insufficient server-side login-attempt limit

------------------------------------------
[Suggested description]

Due to insufficient server-side login-attempt limit enforcement, a vulnerability in /account/login in Huntflow Enterprise before 3.10.14 co

------------------------------------------

[Additional Information]

Example login request to /account/login:

POST /account/login HTTP/1.1
Host: hf.mydomain
Connection: close
Content-Length: 98
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://hf.mydomain
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q
Referer: https://hf.mydomain/account/login
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: lang=ru_RU; _xsrf=2|b65eb986|309cc18c34ff994a04ca856397c5f300|1619468100; token=5kafeoqj6vk2tb3mmx31wyl8zvc1ti7mtfpkretj2k38qgdaddl

_xsrf=2%7Cb65eb986%7C309cc18c34ff994a04ca856397c5f300%7C1619468100&email=user123&password=p@ssw0rd

There is no any server-side login-attempt limit and attacker can perform multiple login attempts for brute-force password guessing.

------------------------------------------

[VulnerabilityType Other]
CWE-307: Improper Restriction of Excessive Authentication Attempts

------------------------------------------

[Vendor of Product]
Huntflow

------------------------------------------

[Affected Product Code Base]
Huntflow Enterprise - Affected < 3.10.14. Fixed at 3.10.14. Tested at 3.6.1

------------------------------------------

[Affected Component]
"/account/login" HTTP method

------------------------------------------

[Attack Type]
Remote - unauthenticated users

------------------------------------------

[CVE Impact]
Brute-force password attacks

------------------------------------------

[Attack Vectors]
To exploit send multiple login attempts to the Huntflow Enterprise "/account/login" HTTP method

------------------------------------------

[Reference]
https://huntflow.ru
https://gist.github.com/andrey-lomtev/4ec9004101152ea9d0043a09d59498a6

------------------------------------------

[Has vendor confirmed or acknowledged the vulnerability?]
true

------------------------------------------
```

```

[Discoverer]
Andrey Lomtev

-----------------------------------------

Andrey Lomtev / Infosec.ru team
```