research@STM:~$ cat /stm/vulndb/CVE-2021-37419

CVE-2021-37419

Name

SSRF vulnerability in /servlet/ADSHACluster endpoint

CVSS score

8.6 (High)

CVSS vector

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

Product name

ManageEngine ADSelfService Plus

Confirmed exploitable versions

< 6112

Researcher

Krzysztof Andrusiak and Marcin Ogorzelski

Description

It is possible to conduct SSRF attack without authentication by sending specially crafted request to `/servlet/ADSHACluster` endpoint. By abusing this vulnerability an attacker can send POST requests to any address, any endpoint and can provide own parameters in POST request body. Requests can be sent via HTTPS protocol only.

Proof-of-concept

1. Start HTTPS server (which will receive POST request sent by ADSSP server).
2. Change the following variables in CVE-2021-37419.py script:
   `ADSSP_URL` - ADSSP server address
   `TARGET_URL` - address to which POST request will be sent (where HTTPS server from step 1 is running)
   `PARAMS` - arguments which will be included in POST request body
3. Execute CVE-2021-37419.py script.
4. HTTPS server from step 1 should receive POST request sent from ADSSP server:

```
[*] Starting HTTPS server on port 8080
[*] Received POST request from 192.168.100.102!
Path: /myOwnAPI
Headers:
Connection: close
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_162
Host: 192.168.100.101:8080
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-type: application/x-www-form-urlencoded
Content-Length: 73
Body:
MTCALL=getHandshakeKey&HANDSHAKE=true&haAuthKey=1&param1=test&param2=test
```

Timeline

- 07-05-2021 - Vulnerability reported to vendor
- 07-05-2021 - First response from vendor
- 24-06-2021 - Update from vendor
- 26-08-2021 - 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#6112

https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6112-hotfix-release