research@STM:~$ cat /stm/vulndb/CVE-2021-3742

CVE-2021-37420

Name
E-mail MIME injection in /RestAPI/PasswordSelfServiceAPI endpoint

CVSS score
6.5 (Medium)

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

Product name
ManageEngine ADSelfService Plus

Confirmed exploitable versions
< 6112

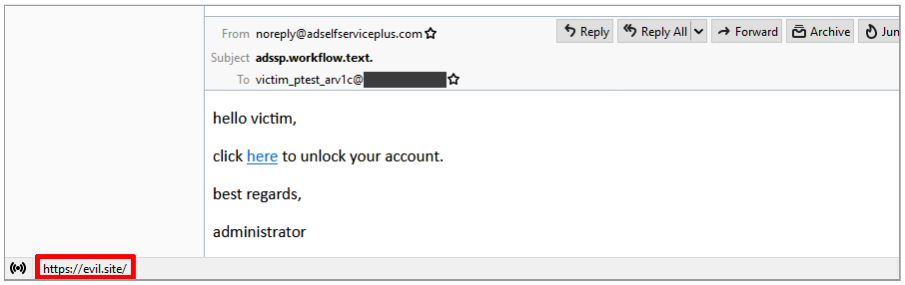
Researcher
Krzysztof Andrusiak and Marcin Ogorzelski

Description

An unauthenticated attacker can send emails with any content to domain users by sending specially crafted requests to "/RestAPI/PasswordSelfServiceAPI" endpoint.

Proof-of-concept

1. Configure mail server in ADSSP.
2. Make sure that "victim" user has e-mail address set in Active Directory.
3. Modify the following parameters in CVE-2021-37420.py script:
   `URL` - ADSSP server URL
   `DOMAIN` - domain name (FQDN)
   `USERNAME` - user from step 2 (AD username, not e-mail address)
   `HTML_CONTENT` - phishing email content
4. Execute CVE-2021-37420.py script - user should receive modified e-mail.



E-mail sent by phishing.py script

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

research@stmcyber.pl