# Subdomain takeover on mta1a1.spmail.uber.com

22

Share:

| | |
|---|---|
| State | Resolved (Closed) |
| Disclosed | **April 7, 2020 3:10am +0530** |
| Reported To | **Uber** |
| Weakness | Improper Access Control - Generic |
| Bounty | $500 |
| Severity | Medium (4 ~ 6.9) |
| Participants | |
| Visibility | Disclosed (Limited) |

Collapse

SUMMARY BY UBER

A dangling AWS record on mta1a1.spmail.uber.com allowed a complete DNS zone takeover, giving an adversary access to mta1a1.spmail.uber.com-scoped cookies and CORS, which could facilitate phishing attacks.

Thanks again, @0x3c3e!

SUMMARY BY 0X3C3E

It's so called IP-use-after-free attack. I was able to obtain an IP address from `mta1a1.spmail.uber.com` **A** DNS record as it was possible to allocate the IP from AWS elastic IP's pool.

> Edit 11/2019 - It would appear AWS has begun serving elastic IPs from a small account-specific pool (similar to GCP). This severly limits the diversity of addresses recieved. (from https://github.com/monoxgas/FlyingAFalseFlag).

As follows from the foregoing, current chances to reproduce something like that should tend to zero.

## References

- Great intro article https://blog.apnic.net/2019/01/09/be-careful-where-you-point-to-the-dangers-of-stale-dns-records/
- AWS elastic IP reference https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html
- BHUSA 2019: Flying a False Flag https://youtu.be/2BEwqbCbQuM?t=1945
- PoC: https://github.com/0x3c3e/recloud
- My quick research https://docs.google.com/spreadsheets/d/18gfOnxFC3rq8Z_Ecnuxdw4ldC79GbzYPqCCn5XX0DVs/

TIMELINE · EXPORT

| | |
|---|---|
| 0x3c3e submitted a report to **Uber**. | Oct 4th (8 months ago) |
| magicmouse HackerOne triage posted a comment. | Oct 5th (8 months ago) |
| magicmouse HackerOne triage updated the severity. | Oct 5th (8 months ago) |
| magicmouse HackerOne triage posted a comment. | Oct 5th (8 months ago) |
| 0x3c3e posted a comment. | Oct 5th (8 months ago) |
| 0x3c3e posted a comment. | Updated Oct 5th (8 months ago) |
| uber_div changed the status to **Triaged**. | Oct 8th (8 months ago) |
| 0x3c3e posted a comment. | Oct 8th (8 months ago) |
| aasthay-uber closed the report and changed the status to **Resolved**. | Oct 9th (8 months ago) |

Uber rewarded 0x3c3e with a **$500** bounty. Oct 22nd (7 months ago)

0x3c3e requested to disclose this report. Dec 16th (6 months ago)

mstroka updated the severity. Apr 7th (2 months ago)

mstroka agreed to disclose this report. Apr 7th (2 months ago)

This report has been disclosed. Apr 7th (2 months ago)