[Mo 04.08.2014 17:30]

Hallo Pascal,

kurz zur Info: Der erste Teilfix wurde heute schon released.
Der vollständige Fix geht morgen Vormittag
live.

Gruß,
  Tilmann

--
Tilmann Haak
Security Engineer

[FR 01.08.2014 10:37]

-- Telko mit kurzer Erläuterung des Problems und möglichen Lösungsvorschlägen --

[Do 31.07.2014 13:57]

Hallo Herr Haak,

alles klar, gerne.

Viele Grüße
Pascal Landau

[Do 31.07.2014 12:13]

Hallo Herr Landau,

vielen Dank für Ihre E-Mail. Ich habe mir den PoC eben kurz angesehen und durchgespielt. Wir werden uns die Problematik heute und morgen einmal näher ansehen.

Ich würde mich dann vermutlich morgen, evtl. auch heute noch kurz bei Ihnen melden.

Viele Grüße,
  Tilmann Haak

--
Tilmann Haak
Security Engineer

XING AG
Dammtorstraße 29-32, 20354 Hamburg, Germany
Tel. +49 40 419131-655, Fax +49 40 419131-11
Commercial Reg. (Registergericht): Amtsgericht Hamburg, HRB 98807

Exec. Board (Vorstand): Dr. Thomas Vollmoeller (Vorsitzender), Ingo Chu, Jens Pape, Timm Richter
Chairman of the Supervisory Board (Aufsichtsratsvorsitzender): Stefan Winners
Please join my network on XING: https://www.xing.com/profile/Tilmann_Haak

This e-mail may contain confidential and/or privileged information. If you are not the intended recipient (or have received this e-mail in error) please notify the sender immediately and destroy this e-mail. Any unauthorised copying, disclosure or distribution of the material in this e-mail is strictly forbidden and may be unlawful.

[Do 31.07.2014 11:23]

Hey Xing Security Team,
I think I have discovered a possible privacy breach exploit on Xing, currently only working in Google Chrome. By bruteforcing profile URLs as a restriction in the Content-Policy-Header it's possible to identify if a user is logged in and **what his exact profile url is**.
Please see http://myseosolution.de/test/csp-deanonymisierung.php?network=Xing&lang=en&token=Eriurbacxnubarcpszz8 for a POC.

Steps to reproduce:

1. Open Google Chrome (25 to 36)
2. Make sure not to block Third-Party-Cookies
3. Log into Xing
4. Enter up to 750 profiles in the text field and make sure to include your own profile *
5. Hit "Start deanonymization"

You should get an output similar to this:

- Starting deanonymization...
- Check: CSP implementation blocks access on path level... **true**
- Check: CSP implementation allows access on path level... **true**
- Check: Logged into Xing... **true**
- Profile found in test group 0? **false**
- Profile found in test group test-set? **true**
- 251 profiles left... decision-tree: **[0]**
- 126 profiles left... decision-tree: **[0,1]**
- 63 profiles left... decision-tree: **[0,1,0]**
- 32 profiles left... decision-tree: **[0,1,0,0]**
- 16 profiles left... decision-tree: **[0,1,0,0,0]**
- 8 profiles left... decision-tree: **[0,1,0,0,0,0]**
- 4 profiles left... decision-tree: **[0,1,0,0,0,0,1]**
- 2 profiles left... decision-tree: **[0,1,0,0,0,0,1,0]**
- 1 profiles left... decision-tree: **[0,1,0,0,0,0,1,0,0]**
- **Profile: https://www.xing.com/[YOUR USERNAME]**

* This step is required for the POC to work, because I did not want to scrape "real" user profiles - not sure about the legal issues that might be involved in mass scraping. In a real world scenario one would use a targeting method to find a predefined set of profiles to check.

Functioning principle in short:
- Content-Security-Header blocks external resources on a _path_ level in Google Chrome
- Use a predefined set of Xing profiles to check if a request to https://www.xing.com/profile resolves
- If yes, split the set of profiles in half and repeat the process, until only one URL is left

Before I write about it, I wanted to check back with you guys if that 'exploit' is something for you to worry about or if it's more or less a "won't fix, go ahead".

Cheers,
Pascal Landau