[Mo 04.08.2014 13:34]

Hi again!

There's no problem on our side, you can publish your article. And of course you can include our responses as well.

Regards,
Krzysztof, Google Security Team

[Mo 04.08.2014 11:14]

Hey Krzysztof,

thank you for your reply. Kinda expected this response :)

One more thing:
As I noted before, I would like to publish a rather detailed article about it (see attachment; it's almost completely tailored to FB).
I checked back with Facebook on this and they gave me their "go" so before I proceed I just wanted to ask for your approval as well.

Plus, can I make a copy of this conversation publicly available (as protocol for the disclosure process)?

Cheers
Pascal

Von: security@google.com [mailto:security@google.com]
Gesendet: Montag, 4. August 2014 10:55
An: pascal.landau@googlemail.com
Betreff: RE: [1-8109000004264] [1-8109000004264] Info Leak in https://plus.google.com/

Hi Pascal!

Thanks for contacting us about the issue. We are aware of the possibility of abusing paths in CSP 1.1 to check whether the user has a given profile ID on various services that include this information in the path. Unfortunately, this is how current version of CSP works. The only fix we can apply here is working on changing the CSP specification in the next version, which we already do. There's an active discussion about it on public-webappsec@w3.org mailing list - see http://lists.w3.org/Archives/Public/public-webappsec/2014Feb/0036.html. You can also track this bug https://code.google.com/p/chromium/issues/detail?id=313737 if you're interested.

Because the issue is known, your report is not eligible for a reward or mention in our Hall of Fame. I do encourage you to keep looking. Good luck on future bug hunting!

Best regards.
Krzysztof, Google Security Team

[Do 31.07.2014 21:54]

Hey - Just letting you know that your report was triaged and we're currently looking into it. You should receive a response in a couple of days, but it might take up to a week if we're particularly busy.

Thanks,
Google Security Team

[Do 31.07.2014 11:19]

Thanks for the vulnerability report.

This email confirms we've received your message. We'll investigate and get back to you once we've got an update.

Cheers,

Google Security Bot

Report Details

Email Subject: [9-9981000004421] Info Leak in https://www.youtube.com/

Category: Info Leak

Product: https://www.youtube.com/

Cid: 9-9981000004421

Hey Google Security Team,
I think I have discovered a possible privacy breach exploit on Youtube, 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 currently logged in and what his exact profile url is. Please see http://myseosolution.de/test/csp-deanonymisierung.php?network=Youtube&lang=en&token=Qbrytdbpkhhzmcxiqim9 for a POC.

1. Open Google Chrome (25 to 36)
2. Make sure not to block Third-Party-Cookies
3. Log into Youtube
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 Facebook... 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.youtube.com/channel/[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 GooglePlus profiles to check if a request to https://www.youtube.com/user 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

PS: This was also send for Google Plus