Privacy Browser - Bug #723

Connects to content-autofill.googleapis.com when tapping on an input field

05/31/2021 06:47 AM - Zounp .

Status:	Closed	**Start date:**	05/31/2021
Priority:	Next Release	**Due date:**	
Assignee:	Soren Stoutner	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

Privacy Browser connects to content-autofill.googleapis.com
Connecting to thirdparty services is not what I expect from a privacy browser.
I think this behaviour must be deleted.

History

#1 - 05/31/2021 08:57 AM - Soren Stoutner

- Priority changed from 3.x to Next Release

I agree that this is very concerning.

What were you doing in the app when it tried to connect to content-autofill.googleapis.com?

What tool are you using to detect that Privacy Browser is attempting to connect to content-autofill.googleapis.com?

#2 - 05/31/2021 02:48 PM - Zounp .

Yes indeed, that is what you need to know.

I use the Netguard firewall on LineageOS 18 (Android 11) to see what is happening.

I will try to reproduce it.
Aha, I think I found it. An website of which I did not expect it.
In the mean time I noticed that, while I was testing with one website, two other domains appeared in the Netguard Privacy Browser section.
Those I have visited before but not while I was testing, nor had they any tabs open and I had Privacy browser exited with the Clear and Exit" section > Clear everything on (active).

I am struggling to understand the exact behavior of Netguard. I need to figure Netguard out before I can continue with reproducing (or not) the findings above.
This can take some time. Expect weeks.

#3 - 05/31/2021 03:00 PM - Soren Stoutner

- File Requests Screenshot.png added

Do you see these connections listed in the Requests section of Privacy Browser (see attached screenshot)? If not, that is very concerning, as Privacy Browser should initiate no network traffic that is not listed there. If you do see it, then the blame likely lies with the web developer of the site you are visiting.

I will keep this bug report open until I hear back from you with further information.

#4 - 05/31/2021 03:07 PM - Zounp .

If you mean: Menu with the 3 horizontal bars > Request-0 then no. I have not seen any entry there as long as I have been using Privacy Browser and looked there.

#5 - 05/31/2021 04:48 PM - Soren Stoutner

- File Autofill Service.png added

I would be interested in any URL that your firewall shows accessing content-autofill.googleapis.com which isn't listed in Requests.

Out of curiosity, are you using an OS level autofill service (see attached screenshot)? If so, have you allowed it access to Privacy Browser (if the OS service is enabled, Privacy Browser's WebView will prompt you if you want to enable it for the app the first time there is a form that can be saved in Autofill)? If so, it wouldn't surprise me that the Autofill service is making network requests to places like content-autofill.googleapis.com, although I would expect that your firewall would indicate that the request is coming from the OS autofill service and not from Privacy Browser. However,

perhaps Autofill somehow indicates to the firewall that the request is being made on behalf of Privacy Browser.

For a little more background on Autofill, see the following two URLs.

https://www.androidcentral.com/how-use-autofill-android-oreo

https://www.stoutner.com/privacy-browser-2-11/

#6 - 05/31/2021 07:16 PM - Zounp .

Thanks for the autofill information.

OS level autofill: No
Settings > Language & input > Autofill service > Autofill service : None

#7 - 05/31/2021 07:29 PM - Soren Stoutner

OK. So, that's definitely not what's going on.

#8 - 05/31/2021 07:30 PM - Soren Stoutner

If you can give me an example URL I would be interested in seeing if I can replicate the behavior. Or, is it happening randomly irrespective of the URLs that are loaded?

#9 - 06/01/2021 05:56 AM - Zounp .

Yes, I can. Giving an URL at this point would be a privacy issue.
I will try if I can reproduce it with an other domain and let you know.

#10 - 06/09/2021 01:47 PM - Soren Stoutner

- Status changed from New to Feedback

#11 - 06/23/2021 03:58 AM - No Name

I analyzed the data traffic: https://www.kuketz-blog.de/privacy-browser-datensendeverhalten-android-app-browser-check-teil11/

Every time the browser finds an input field on a web page, it apparently opens a connection to the address **content-autofill.googleapis.com**. Why an autofill service for forms needs to initiate a connection to Google is beyond me. I almost suspect that the call comes about because the Privacy Browser uses the System WebView to display web pages and this causes the call.

HTTP-Request:

```
GET /v1/pages/ChNDaHJvbWUvOTAuMC40NDMwLjgyEhAJ07mi3Bp4sQoSBQ27V1Zq?alt=proto HTTP/1.1
Host: content-autofill.googleapis.com
Connection: close
X-Goog-Encode-Response-If-Executable: base64
X-Goog-Api-Key: dummytoken
Sec-Fetch-Site: none
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
User-Agent: Mozilla/5.0 (Linux; Android 10; Mi A1 Build/QQ3A.200805.001; wv) AppleWebKit/537.36 (KHTML, like G
ecko) Version/4.0 Chrome/90.0.4430.82 Mobile Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7
```

HTTP-Response :

```
HTTP/1.1 400 Bad Request
Vary: Origin
Vary: X-Origin
Vary: Referer
Content-Type: application/x-protobuf
Date: Sun, 20 Jun 2021 18:02:13 GMT
Server: ESF
Cache-Control: private
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,
h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"
Connection: close
Content-Length: 166
```

```
/API key not valid. Please pass a valid API key.q
(type.googleapis.com/google.rpc.ErrorInfoE
API_KEY_INVALIDgoogleapis.com"
serviceautofill.googleapis.com
```

You can reproduce the behaviour if you visit my blog: www.kuketz-blog.de

The search field triggers the connection to "autofill-content.googleapis.com".

#12 - 06/23/2021 08:09 AM - Soren Stoutner

- Subject changed from Connects to Google services to Connects to content-autofill.googleapis.com when tapping on an input field

Thanks for the additional information, which is very helpful. I am currently on vacation and won't be back to the equipment I need to try to replicate the issue until the end of the week. But I have a few questions that might provide useful information.

1. What program are you using to detect the information about the HTTP request and response information? Is it a firewall on your device or a network level proxy?
2. What settings do you have for the OS Autofill service (described above)?
3. Do you see the same behavior with another browser based on WebView like Lightning (https://f-droid.org/en/packages/acr.browser.lightning/)?
4. Do you see the same behavior with a browser based on Gecko like Fennec (https://f-droid.org/en/packages/org.mozilla.fennec_fdroid/)?
5. If you have root on your device, do you see this behavior if you replace the default WebView with Bromite's SystemWebView (https://www.bromite.org/system_web_view.html)?
6. Please post a copy of your About > Version. It is possible that this only affects certain ROMs, versions of Android, or versions of WebView.

#13 - 06/24/2021 12:05 AM - No Name

1. I use a network proxy - BurpSuite.
2. Under "System ~~> Languages, inputs & gestures~~ > Advanced -> Autofill services" I selected "No App".
3. Yes, I do.
4. No.
5. I won't change that right now. Sorry.
6. Here are the details:
Android-Version: 10
LineageOS-Version: 17.1-202106622-NIGHTLY-tissot
LineageOS API-Level: llama (9)
Security level: 5. June
Kernel-Version: 4.9.188-perf+

It's a Xiaomi Mi A1 test device.

#14 - 06/24/2021 12:10 AM - No Name

I want to add my WebView version: 91.0.4472.101

#15 - 06/24/2021 06:39 AM - Zounp .

Tested once more:
Autofill status: Settings > System > Languages & inputs > Advanced > Autofill service: None
Went to startpage.com.

Privacy browser:

- Nicely transforms it to https://startpage.com
- Search suggestions appeared. I did not allow content-autofill.googleapis.com in Netguard.
- When I look in Netguard I see connection attempts on TCP4 & -6 to content-autofill.googleapis.com

Smartcookieweb:

- Same behaviour: Wants to go to content-autofill.googleapis.com.
- Search suggestions appeared. I did not allow content-autofill.googleapis.com in Netguard.

Fennec:

- No extra connections appeard in Netguard. Only to startpage.com
- Search suggestions appeared. I did not allow content-autofill.googleapis.com in Netguard.

#16 - 06/26/2021 10:09 AM - Soren Stoutner

I am not able to replicate the issue on the following device:

Privacy Browser
Version 3.8 (version code 55)

Hardware
Brand: google
Manufacturer: Google
Model: Pixel 5
Device: redfin
Bootloader: r3-0.3-7241848
Radio: g7250-00132-210419-B-7294132,g7250-00132-210419-B-7294132

Software
Android: 11 (API 30)
Security Patch: 2021-06-05
Build: RQ3A.210605.005
WebView Provider: com.google.android.webview
WebView Version: 91.0.4472.120
Orbot: 16.4.1-RC-2-tor.0.4.4.6
I2P: 0.9.49
OpenKeychain: 5.7.5

Memory Usage
App Consumed Memory: 13.01 MiB
App Available Memory: 27.43 MiB
App Total Memory: 40.44 MiB
App Maximum Memory: 256.00 MiB
System Consumed Memory: 3,439.48 MiB
System Available Memory: 4,018.25 MiB
System Total Memory: 7,457.73 MiB

Blocklists
EasyList: 202105211708
EasyPrivacy: 202105211708
Fanboy's Annoyance List: 202105212100
Fanboy's Social Blocking List: 202105211708
UltraList: 1
UltraPrivacy: 2

Package Signature
Issuer DN: CN=Android Debug, O=Android, C=US
Subject DN: CN=Android Debug, O=Android, C=US
Start Date: Mar 11, 2015 12:39:21 PM MST
End Date: Mar 3, 2045 12:39:21 PM MST
Certificate Version: 3
Serial Number: 372300976
Signature Algorithm: SHA256withRSA

Specifically, no DNS lookups were ever made to content-autofill.googleapis.com while browsing startpage.com and www.kuketz-blog.de, tapping on a field, and doing a search using either Privacy Browser or Lightning.

As both of the people who are experiencing this problem are running LineageOS, I wonder if the issue is with some modification to that ROM. Do either of you have the ability to test a vanilla Android device?

#17 - 06/29/2021 01:30 AM - No Name

With the FOSS Browser (https://github.com/scoute-dich/browser) I won't see connections to content-autofill.googleapis.com.

The browser also uses Android System WebView.

#18 - 06/29/2021 06:18 AM - Soren Stoutner

Do you see connections to content-autofill.googleapis.com on any device not running LineageOS?

#19 - 07/06/2021 01:51 PM - Soren Stoutner

- Status changed from Feedback to Closed

Based on the information that has been provided so far, it appears that something like the following is happening:

1. A user taps on a field on a webpage in Privacy Browser.
2. WebView asks the Autofill service if it would like to provide autofill information.
3. Autofill sees that the None service is selected. On standard Android, Autofill does nothing. However, on LineageOS Autofill sends a request to content-autofill.googleapis.com with `X-Goog-Api-Key: dummytoken`.

It is unclear why LineageOS is doing this. It is likely due to some change they have made to the OS that has this unintended consequence.

Whatever the reason, based on the information above, it appears that this bug should actually be filed with LineageOS instead of with Privacy Browser. As such, I am closing the bug report. Feel free to add a comment if you have any indication that this behavior occurs on ROMs not based

on LineageOS and I will reopen the bug.

#20 - 09/27/2021 08:54 AM - Soren Stoutner

This bug report is mentioned at https://gitlab.com/fdroid/fdroiddata/-/merge_requests/9655#note_687142404 because, of course, it affects any app using WebView on a LineageOS device.

Files

Requests Screenshot.png	141 KB	05/31/2021	Soren Stoutner
Autofill Service.png	53.2 KB	05/31/2021	Soren Stoutner