Closed · Issue created 2 years ago by lovetox

(CVE-2020-6750) Socks5 Proxy: Proxy on a SocketClient set via set_proxy_resolver ignored

Hi,

GLib Version: 2.62.0

Im seeing in my client that 5 times out of 10 the proxy set via SocketClient.set_proxy_resolver() is simply ignored without any error whatsoever, and SocketClient just connects to the destination address without proxy.

I would consider this a big privacy/security issue.

Maybe someone can try to reproduce this themself

from my application logs it looks like this

```
23:16:56 INFO    nbxmpp.tcp         Set Proxy: socks5://37.120.155.227:1080
**<Gio.SimpleProxyResolver object at 0x7f77d8bc89b0 (GSimpleProxyResolver at 0x2c8a0d0)>**
23:16:56 INFO    nbxmpp.tcp         Try to connect to 2a03:4000:34:3a4:::5223
23:16:56 INFO    nbxmpp.connection  Set Connection State: TCPState.CONNECTING
<Gio.SocketClient object at 0x7f77d8bc82d0 (GSocketClient at 0x2b666e0)> <enum G_SOCKET_CLIENT_RESOLVING of type Gio.SocketClientEve
<Gio.SocketClient object at 0x7f77d8bc82d0 (GSocketClient at 0x2b666e0)> <enum G_SOCKET_CLIENT_RESOLVED of type Gio.SocketClientEven
<Gio.SocketClient object at 0x7f77d8bc82d0 (GSocketClient at 0x2b666e0)> <enum G_SOCKET_CLIENT_CONNECTING of type Gio.SocketClientEv
<Gio.SocketClient object at 0x7f77d8bc82d0 (GSocketClient at 0x2b666e0)> <enum G_SOCKET_CLIENT_RESOLVING of type Gio.SocketClientEve
<Gio.SocketClient object at 0x7f77d8bc82d0 (GSocketClient at 0x2b666e0)> <enum G_SOCKET_CLIENT_CONNECTED of type Gio.SocketClientEve
<Gio.SocketClient object at 0x7f77d8bc82d0 (GSocketClient at 0x2b666e0)> <enum G_SOCKET_CLIENT_COMPLETE of type Gio.SocketClientEven
**True**
**<Gio.SimpleProxyResolver object at 0x7f77d8bc89b0 (GSimpleProxyResolver at 0x2c8a0d0)>**
23:16:56 INFO    nbxmpp.connection  Set Connection State: TCPState.CONNECTED
23:16:56 INFO    nbxmpp.connection  Signal: connected
```

I made sure that proxy-enabled is set, and made sure the SimpleProxyResolver object is set on the SocketClient, before and after connecting to the server.

I happy to provide more info if needed

Edited 2 years ago by Michael Catanzaro

Drag your designs here or click to upload.

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Related merge requests 2

qsocketclient: Refactor g_socket_client_connect_async()
!1339 · 2.62.5

Refactor g_socket_client_connect_async()
!1365 · 2.62.5

When these merge requests are accepted, this issue will be closed automatically.

Activity

Philip Withnall added GProxy GSocket labels 2 years ago

Philip Withnall @pwithnall · 2 years ago · Maintainer

@mcatanzaro, @pgriffis, any ideas? This might have changed with the Happy Eyeballs stuff, or it might be a completely unrelated bug.

lovetox @lovetox · 2 years ago · Author

It is unrelated to happy eyeballs because i dont use the SocketClient resolver, i resolve my domains myself, and feed only the IP to socketclient, i see this happen for IPV4 and IPV6 alike.

Note: Dont know why the SocketClient issues resolving events.

What i saw in Wireshark, is that a Socks request got mangled with my first data that i write after connection finished. So i think there is some race condition there, feels like, it enters the proxy code, but at the same time socket client continues without proxy.

Michael Catanzaro @mcatanzaro · 2 years ago · Maintainer

> It is unrelated to happy eyeballs because i dont use the SocketClient resolver, i resolve my domains myself, and feed only the IP to socketclient, i see this happen for IPV4 and IPV6 alike.

It's still going through the Happy Eyeballs code. We still feed the IPs into GSocketAddressEnumerator. Please go back to GLib 2.58 and test there; does it work? If so, it's a Happy Eyeballs regression.

If you can figure out if this used to work and broke recently, that'd be really helpful.

Please also post sample code, so we can test for ourselves and determine whether we need to request a CVE (very likely).

Philip Withnall made the issue confidential 2 years ago

Philip Withnall added 2. Needs Information label 2 years ago

lovetox @lovetox · 2 years ago · Author

So here is the sample script, only python, but this should make it easy to port it to C if you need that

The IPs in the script are functional servers you can use to test against

SOCKS is a NordVPN socks5 proxy

DEST_IP is my XMPP Server

```
import sys

from gi.repository import Gio
from gi.repository import GObject
from gi.repository import GLib

DEST_IP = '194.59.207.70'
DEST_PORT = 5223

DEST_IP_V6 = '2a03:4000:34:3a4::'

SOCKS_IP = '37.120.155.227'
SOCKS_PORT = 1080

SOCKS_URI = 'socks5://%s:%s' % (SOCKS_IP, SOCKS_PORT)

resolver = Gio.SimpleProxyResolver.new(SOCKS_URI, None)

print('ProxyResolver: ', resolver)

client = Gio.SocketClient.new()
client.set_proxy_resolver(resolver)
GObject.Object.connect(client, 'event', print)

con = None

def connect():
    print('Try to connect to %s:%s over %s:%s' % (DEST_IP_V6, DEST_PORT, SOCKS_IP, SOCKS_PORT))

    client.connect_async(Gio.InetSocketAddress.new_from_string(DEST_IP_V6, DEST_PORT),
                         None,
                         _on_connect,
```

```
                        None)

def _on_connect(socket_client, result, _user_data):
    global con
    try:
        con = socket_client.connect_finish(result)
    except GLib.Error as error:
        print(error)
        sys.exit()
        return

    print('Successful connected to Destination: %s:%s' % (DEST_IP_V6, DEST_PORT))

    print('Check SocketClient.enable-proxy": ', socket_client.props.enable_proxy)
    print('Check SocketClient.proxy-resolver": ', socket_client.props.proxy_resolver)


connect()
GLib.MainLoop().run()
```

Its not easy to reproduce this, today it took me 10 minutes, i think you need a bad WLAN or Mobile connection. Which could hint at some resolver code.

After 10 minutes of running the script and changing WLAN until i hit the sweetspot and the third try here reproduced the problem

```
philipp@lovetox:~/projects/tests$ python3 test1.py
ProxyResolver:  <Gio.SimpleProxyResolver object at 0x7f8198b92410 (GSimpleProxyResolver at 0x19a3660)>
Try to connect to 2a03:4000:34:3a4:::5223 over 37.120.155.227:1080
<Gio.SocketClient object at 0x7f8198b92aa0 (GSocketClient at 0x18bab40)> <enum G_SOCKET_CLIENT_RESOLVING of type Gio.Socke
<Gio.SocketClient object at 0x7f8198b92aa0 (GSocketClient at 0x18bab40)> <enum G_SOCKET_CLIENT_RESOLVED of type Gio.Socket
<Gio.SocketClient object at 0x7f8198b92aa0 (GSocketClient at 0x18bab40)> <enum G_SOCKET_CLIENT_CONNECTING of type Gio.Soci
<Gio.SocketClient object at 0x7f8198b92aa0 (GSocketClient at 0x18bab40)> <enum G_SOCKET_CLIENT_CONNECTED of type Gio.Socke
<Gio.SocketClient object at 0x7f8198b92aa0 (GSocketClient at 0x18bab40)> <enum G_SOCKET_CLIENT_PROXY_NEGOTIATING of type (
<Gio.SocketClient object at 0x7f8198b92aa0 (GSocketClient at 0x18bab40)> <enum G_SOCKET_CLIENT_RESOLVING of type Gio.Socke
<Gio.SocketClient object at 0x7f8198b92aa0 (GSocketClient at 0x18bab40)> <enum G_SOCKET_CLIENT_COMPLETE of type Gio.Socket
g-io-error-quark: The SOCKSv5 proxy requires an authentication method that is not supported by GLib. (41)


philipp@lovetox:~/projects/tests$ python3 test1.py
ProxyResolver:  <Gio.SimpleProxyResolver object at 0x7fa37362c5a0 (GSimpleProxyResolver at 0x24ee660)>
Try to connect to 2a03:4000:34:3a4:::5223 over 37.120.155.227:1080
<Gio.SocketClient object at 0x7fa37362cbe0 (GSocketClient at 0x2405b40)> <enum G_SOCKET_CLIENT_RESOLVING of type Gio.Socke
<Gio.SocketClient object at 0x7fa37362cbe0 (GSocketClient at 0x2405b40)> <enum G_SOCKET_CLIENT_RESOLVED of type Gio.Socket
<Gio.SocketClient object at 0x7fa37362cbe0 (GSocketClient at 0x2405b40)> <enum G_SOCKET_CLIENT_CONNECTING of type Gio.Soci
<Gio.SocketClient object at 0x7fa37362cbe0 (GSocketClient at 0x2405b40)> <enum G_SOCKET_CLIENT_CONNECTED of type Gio.Socke
<Gio.SocketClient object at 0x7fa37362cbe0 (GSocketClient at 0x2405b40)> <enum G_SOCKET_CLIENT_PROXY_NEGOTIATING of type (
<Gio.SocketClient object at 0x7fa37362cbe0 (GSocketClient at 0x2405b40)> <enum G_SOCKET_CLIENT_RESOLVING of type Gio.Socke
<Gio.SocketClient object at 0x7fa37362cbe0 (GSocketClient at 0x2405b40)> <enum G_SOCKET_CLIENT_COMPLETE of type Gio.Socket
g-io-error-quark: The SOCKSv5 proxy requires an authentication method that is not supported by GLib. (41)


philipp@lovetox:~/projects/tests$ python3 test1.py
ProxyResolver:  <Gio.SimpleProxyResolver object at 0x7f6a3c4db5a0 (GSimpleProxyResolver at 0xfa3660)>
Try to connect to 2a03:4000:34:3a4:::5223 over 37.120.155.227:1080
<Gio.SocketClient object at 0x7f6a3c4dbc30 (GSocketClient at 0xebab40)> <enum G_SOCKET_CLIENT_RESOLVING of type Gio.Socket
<Gio.SocketClient object at 0x7f6a3c4dbc30 (GSocketClient at 0xebab40)> <enum G_SOCKET_CLIENT_RESOLVED of type Gio.Socket(
<Gio.SocketClient object at 0x7f6a3c4dbc30 (GSocketClient at 0xebab40)> <enum G_SOCKET_CLIENT_CONNECTING of type Gio.Socke
<Gio.SocketClient object at 0x7f6a3c4dbc30 (GSocketClient at 0xebab40)> <enum G_SOCKET_CLIENT_RESOLVING of type Gio.Socket
<Gio.SocketClient object at 0x7f6a3c4dbc30 (GSocketClient at 0xebab40)> <enum G_SOCKET_CLIENT_CONNECTED of type Gio.Socket
<Gio.SocketClient object at 0x7f6a3c4dbc30 (GSocketClient at 0xebab40)> <enum G_SOCKET_CLIENT_COMPLETE of type Gio.Socket(
Successful connected to Destination: 2a03:4000:34:3a4:::5223
Check SocketClient.enable-proxy":  True
Check SocketClient.proxy-resolver":  <Gio.SimpleProxyResolver object at 0x7f6a3c4db5a0 (GSimpleProxyResolver at 0xfa3660)
```

Edited by lovetox 2 years ago

lovetox @lovetox · 2 years ago — Author

Because of the nature of the problem, i think i can only prove that a problem exists with a certain GLib version, but not the opposite

I can reproduce currently with 2.62.0

i think the order of events is maybe a hint, if i would take a stab in the dark, the second RESOLVING event could be the start of the problem

Edited by lovetox 2 years ago

lovetox changed the description 2 years ago

Michael Catanzaro @mcatanzaro · 2 years ago — Maintainer

I think I found the bug. data->proxy_addr gets cleared at the start of enumerator_next_async() and not set again until name resolution has completed in g_socket_client_enumerator_callback(). Say we have a successful name resolution and then start connecting to the resolved address, at the bottom of g_socket_client_enumerator_callback(). Then we hit the happy eyeballs timeout on that connection attempt and begin resolving a new address, clearing data->proxy_addr. Then the connection attempt succeeds. Boom, GLib has forgotten that it is supposed to connect to the proxy! It would be a regression since 2.60 and definitely warrants a CVE.

This might also explain what's going on in two or three other GSocketClient bugs.

Edited by Michael Catanzaro 2 years ago

Michael Catanzaro mentioned in issue #1995 (closed) 2 years ago

lovetox @lovetox · 2 years ago — Author

Great job! Im glad you seem to have found the problem, such bugs are really a nightmare to debug.

Michael Catanzaro removed ? Needs Information label 2 years ago

Michael Catanzaro made the issue visible to everyone 2 years ago

Michael Catanzaro @mcatanzaro · 2 years ago — Maintainer

Making this public since it's not exploitable and we're going to need to warn users.

Michael Catanzaro mentioned in issue #1902 (closed) 2 years ago

Michael Catanzaro @mcatanzaro · 2 years ago — Maintainer

> definitely warrants a CVE

I'll request one.

Michael Catanzaro changed title from **Socks5 Proxy: Proxy on a SocketClient set via set_proxy_resolver ignored** to **(CVE-2020-6750) Socks5 Proxy: Proxy on a SocketClient set via set_proxy_resolver ignored** 2 years ago

Michael Catanzaro changed milestone to %2.62.5 2 years ago

Patrick Griffis mentioned in merge request !1339 (merged) 2 years ago

Patrick Griffis mentioned in commit 760de95e 2 years ago

Patrick Griffis mentioned in commit ddc494a8 2 years ago

Patrick Griffis mentioned in commit ab8800ab 2 years ago

Michael Catanzaro @mcatanzaro · 2 years ago — Maintainer

Hi lovetox, if you're willing to rebuild glib, it'd be great if you could test !1339 (merged). I think it should resolve this issue, but there's no better way to be sure than for the reporter to confirm. :)

Patrick Griffis mentioned in commit b875102a 2 years ago

Patrick Griffis mentioned in commit d4fcf914 2 years ago

Patrick Griffis mentioned in commit e2cb85a8 2 years ago

Patrick Griffis mentioned in commit 2722620e 2 years ago

Patrick Griffis closed via commit 2722620e 2 years ago

Philip Withnall closed via commit dff212ef 2 years ago

Patrick Griffis mentioned in commit 664afb2b 2 years ago

Michael Catanzaro mentioned in merge request !1365 (merged) 2 years ago

Patrick Griffis mentioned in commit 08677ed5 2 years ago

Philip Withnall mentioned in commit dff212ef 2 years ago