

(CVE-2020-13645) GTlsClientConnection silently ignores unset server identity

When the server-identity property of GTlsClientConnection is unset, the documentation says we need to fail the certificate verification with G_TLS_CERTIFICATE_BAD_IDENTITY:

If the G_TLS_CERTIFICATE_BAD_IDENTITY flag is set in "validation-flags", this object will be used to determine the expected identity of the remote end of the connection; if "server-identity" is not set, or does not match the identity presented by the server, then the G_TLS_CERTIFICATE_BAD_IDENTITY validation will fail.

This is important because otherwise, it's easy for applications to fail to specify server identity. When server identity is missing, we check the validity of the TLS certificate but do not check if it corresponds to the expected server. That is, evil.com can present a valid certificate issued to evil.com, and we will happily accept it for paypal.com.

This was discovered in [balsa#34 \(closed\)](#).

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

[Return bad identity error if identity is unset](#)

1123

✓


[Improve documentation of g_tls_database_verify_chain\(\)](#)


glib#1475


⚠️

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

Activity

 **Michael Catanzaro** added [1 Bug](#), [1 Security](#), [5 GnuTLS](#), [5 OpenSSL](#) labels [2 years ago](#)


 **Michael Catanzaro** mentioned in issue [balsa#34 \(closed\)](#) [2 years ago](#)


 **Michael Catanzaro** @mcatanzaro · [2 years ago](#)


Author


Maintainer


Note that while the connection API is supposed to be fail-safe, the GTlsCertificate and GTlsDatabase APIs are the opposite (no identity means identity not checked) since those are used outside the context of a TLS connection. The documentation for GTlsCertificate already indicates this, but the documentation GTlsDatabase does not describe the behavior either way. Fixed this in [glib#1475 \(merged\)](#).


 **Michael Catanzaro** removed [5 GnuTLS](#), [5 OpenSSL](#) labels [2 years ago](#)


 **Michael Catanzaro** mentioned in issue [#130 \(closed\)](#) [2 years ago](#)


 **Michael Catanzaro** changed title from [g_tls_database_gnutls_verify_chain/g_tls_database_openssl_verify_chain silently ignore unset server identity](#) to [GTlsClientConnection silently ignores unset server identity](#) [2 years ago](#)


 **Michael Catanzaro** changed the description [2 years ago](#)


 **Michael Catanzaro** mentioned in commit [ed41e68f](#) [2 years ago](#)

 **Michael Catanzaro** mentioned in merge request [1123 \(merged\)](#) [2 years ago](#)

 **Michael Catanzaro** mentioned in commit [f4b4b7eb](#) [2 years ago](#)

 **Michael Catanzaro** mentioned in commit [ddc25dc9](#) [2 years ago](#)

 **Michael Catanzaro** mentioned in commit [d9c8d69f](#) [2 years ago](#)

 **Michael Catanzaro** @mcatanzaro · [2 years ago](#)


Author

Maintainer

So this is CWE-297: "Improper Validation of Certificate with Host Mismatch." Hi [@d-hat](#), I think this merits a CVE. Is that something you can help with, or should I request via MITRE?


Suggested description: "glib-networking's implementations of GTlsClientConnection, prior to version 2.64.3, would skip hostname verification of the server's TLS certificate if the application failed to specify the expected server identity. This is in contrast to its intended documented behavior, to fail the certificate verification. Applications that failed provide the server identity, including the balsa email client, would accept TLS certificates if the certificate is valid for any host."


I did a Debian codesearch, and balsa is the only application that's passing a NULL literal, so it's *probably* the only affected application in distros. See also: [balsa#34 \(comment 789872\)](#).

 **d-hat** @d-hat · [2 years ago](#)

Reporter

CVE assignment will have to come from MITRE. The description and CWE look good 🍀

 **Michael Catanzaro** closed via commit [d9c8d69f](#) [2 years ago](#)

 **Michael Catanzaro** @mcatanzaro · [2 years ago](#)

Author


Maintainer


CVE assignment will have to come from MITRE.

I'm seeing an invalid TLS certificate on [https://cveform.mitre.org/](#). It's not a MITM because the site works in Firefox; they've just messed up their web server configuration. They are sending only a server cert with no chain of trust, so validation is guaranteed to fail. (Firefox has the intermediate certificate cached from a previous page load; it fails to load there too if I delete my ~/mozilla and start fresh.)

```
$ gnutls-cli cveform.mitre.org
Processed 157 CA certificate(s).
Resolving 'cveform.mitre.org:443'...
Connecting to '198.49.146.153:443'...
- Certificate type: x.509
- Get a certificate list of 1 certificates.
- Certificate[0] info:
  - subject 'CN=cveform.mitre.org,O=The Mitre Corporation,L=McLean,ST=Virginia,C=US', issuer 'CN=Entrust Certification Authority
    Public Key ID:
      sha1:8c228c9b43f8dc6f3328f531feb02115f178dc91
      sha256:84298651266ef5e60ccedf0bc104878a771b0d90f53c2e68b549d4d587250ff
    Public Key PIN:
      pin-sha256:hCnGUSZu9eYw7N8LWQSHlnchj2D1PC5oy1SdVtHy6PB=
- Status: The certificate is NOT trusted. The certificate issuer is unknown.
*** PKI verification of server certificate failed...
*** Fatal error: Error in the certificate.
```

So I will not request a CVE from MITRE right now.


 **Michael Catanzaro** mentioned in commit [29513046](#) [2 years ago](#)

 **Michael Catanzaro** @mcatanzaro · [2 years ago](#)

Author

Maintainer

The CVE request form is still broken, so I have contacted MITRE to inform them.

 **Michael Catanzaro** @mcatanzaro · [2 years ago](#)

Author

Maintainer

MITRE has not responded to my request to fix the CVE request form. So if Red Hat is no longer assigning CVEs, we will likely have to go without for this issue, at least for the foreseeable future.



Michael Catanzaro @mrcatanzaro · 2 years ago

Author

Maintainer

I was hoping to get a CVE assignment first to put in the release NEWS before making a release with the fix, but no response yet from MITRE, so we'll probably go without. [Blog post](#)



Michael Catanzaro changed title from `GTlsClientConnection silently ignores unset server identity` to `(CVE-2020-13645) GTlsClientConnection silently ignores unset server identity` 2 years ago



Michael Catanzaro @mrcatanzaro · 2 years ago

Author

Maintainer

Someone anonymous requested a CVE, we got CVE-2020-13645.

The CVE request form is still broken though, so the underlying problem remains.



Michael Catanzaro @mrcatanzaro · 2 years ago

Author

Maintainer

The CVE request form is still broken though, so the underlying problem remains.

Now it's fixed. Thanks whoever got in touch with MITRE.

Please [register](#) or [sign in](#) to reply