New issue

Jump to bottom

# Axel may not verify server certificate CN/SAN/hostname (allowing SSL interception) #262

Closed **theopolis** opened this issue on Mar 16, 2020 · 0 comments · Fixed by Jason23347/axel#1

Labels bug

Milestone v2.17.8

**theopolis** commented on Mar 16, 2020 Contributor

It looks like Axel's SSL's connections do not verify server certificate hostnames. To fix this the SSL context should set a certificate callback or use `SSL_set1_host` to set the intended hostname.

This is an issue since it uses `SSL_CTX_set_default_verify_paths` and loads all root authorities from the OS. See https://wiki.openssl.org/index.php/Hostname_validation for a description of this nuance with the OpenSSL APIs.

Here is potentially insecure code
https://github.com/axel-download-accelerator/axel/blob/master/src/ssl.c#L83

```
[...]
ssl_ctx = SSL_CTX_new(SSLv23_client_method());
if (!conf->insecure) {
    SSL_CTX_set_default_verify_paths(ssl_ctx);
    SSL_CTX_set_verify(ssl_ctx, SSL_VERIFY_PEER, NULL);
}
SSL_CTX_set_mode(ssl_ctx, SSL_MODE_AUTO_RETRY);

ssl = SSL_new(ssl_ctx);
SSL_set_fd(ssl, fd);
SSL_set_tlsext_host_name(ssl, hostname);

int err = SSL_connect(ssl);
if (err <= 0) {
[...]
```

**theopolis** mentioned this issue on Mar 16, 2020

**SSL add hostname verification** #263

Closed

**ismaell** modified the milestones: **v3.0**, **v2.18** on Mar 17, 2020

**ismaell** added the bug label on Mar 17, 2020

**ismaell** modified the milestones: **v2.18**, **v2.17.8** on Mar 17, 2020

**ismaell** closed this as completed in 961cf54 on Mar 23, 2020

**Jason23347** mentioned this issue on Mar 23, 2020

**SSL: Add hostname verification** Jason23347/axel#1

Merged

**davidpolverari** pushed a commit to davidpolverari/axel that referenced this issue on Aug 26, 2021

`SSL: Add hostname verification` ··· `f37b41e`

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

v2.17.8

Development

Successfully merging a pull request may close this issue.

**SSL: Add hostname verification**

axel-download-accelerator/axel

**SSL add hostname verification**

theopolis/axel

---

2 participants