ounties Research Advisories Get Involved Events

## GHSL-2020-097: Missing hostname validation in twitter-stream - CVE-2020-24392



#### Summary

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

### Product

### Tested Version

v0.1.16

#### Details

Missing SSL/TLS certificate hostname validation

 $\underline{\text{twitter-stream}} \text{ uses the library } \underline{\text{eventmachine}} \text{ in an insecure way that allows an attacker to perform a monster in the middle attack against users of the library } \underline{\text{eventmachine}} \text{ in an insecure way that allows an attacker to perform a monster in the middle attack against users of the library } \underline{\text{eventmachine}} \text{ in an insecure way that allows an attacker to perform a monster in the middle attack against users of the library } \underline{\text{eventmachine}} \text{ in an insecure way that allows an attacker to perform a monster in the middle attack against users of the library } \underline{\text{eventmachine}} \text{ in an insecure way that allows an attacker to perform a monster in the middle attack against users of the library } \underline{\text{eventmachine}} \text{ in an insecure way that allows an attacker to perform a monster in the middle attack against users of the library } \underline{\text{eventmachine}} \text{ in an insecure way that allows an attacker to perform a monster in the middle attack against users of the library } \underline{\text{eventmachine}} \text{ in an insecure way that } \underline{\text{eventmachine}} \text{ in an insecure way that } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in an insecure way that } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in a minute of the library } \underline{\text{eventmachine}} \text{ in$ 

#### Impact

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

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
```

# openael reg = 1509 -menkey rea:2048 + seyout key.pem -out cart.pem -days 369 -modes
# Listano np. port 44 with Tist canabled.
# openael s server -key key.pem -cart cert.pem -accept 443
Using auto Tip Farameters
# Cart Cart.pem -accept 443
Using auto Tip Farameters
# Cart.pem -acc

#### Create a sample client with the following contents:

```
require 'rubygems'
require 'twitter/json_stream'
EventMachine::run |
stream = Twitter::SONStream.connect(
:path => '/1.1/statuses/filter.json',
:auth => 'USERNAME:SECRETPASSWORD'
  stream.each_item do |item|
  stream.on_error do |message|
end
  stream.on max reconnects do |timeout, retries|
```

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

\$ ruby twitter-stream.rb

CWE-297: Improper Validation of Certificate with Host Mismatch

#### CVE

## **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-2020-097 in any communication regarding this issue.

## GitHub

## Product

## Platform

# Support

### Company

- About
   Blog
   Carcers
   Press
   Shop
   If

- © 2021 GitHub, Inc.
   Terms
   Privacy
   Cookie settings