New issue

Jump to bottom

Security vulnerability: missing SSL hostname validation #339

Closed igrigorik opened this issue on May 24, 2020 · 10 comments · Fixed by #340

igrigorik commented on May 24, 2020 Owner

GitHub Security Lab (GHSL) Vulnerability Report: `GHSL-2020-094`

Summary

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

Product

em-http-request

Tested Version

1.1.5

Missing SSL/TLS certificate hostname validation

em-http-request uses the library eventmachine in an insecure way that allows an attacker to perform a man 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.

Remediation

Implement hostname validation.

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 test.coinbase.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-----
MGoCAQECAgMDBALAMAQABDDtsipRTslOpunNYATFLBo/Urf61flD0RYbyS0cpgwt
cH5uPqX4CKfCYg196MsV+HehBgIEXrqnkKIEAgIcIKQGBAQBAAAAphMEEXRlc3Qu
Y29pbmJhc2UuY29t
-----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:
CIPHER is ECDHE-RSA-AES256-GCM-SHA384
Secure Renegotiation IS supported
GET / HTTP/1.1
Connection: close
Host: test.coinbase.com
User-Agent: EventMachine HttpClient
Accept-Encoding: gzip, compressed
```

Create a sample client with the following contents:

```ruby
require 'rubygems'
require 'eventmachine'
require 'em-http'

urls = ARGV
if urls.size < 1
  puts "Usage: #{$0} <url> <url> <...>"
  exit
end

pending = urls.size

EM.run do
  urls.each do |url|
    http = EM::HttpRequest.new(url).get
    http.callback {
      puts "#{url}\n#{http.response_header.status} - #{http.response.length} bytes\n"
      puts http.response

      pending -= 1
      EM.stop if pending < 1
    }
```

```
    http.errback {
      puts "#{url}\n" + http.error

      pending -= 1
      EM.stop if pending < 1
    }
  end
end
```

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

```
$ ruby em-http-request-client.rb "https://test.coinbase.com"
```

References

CWE-297: Improper Validation of Certificate with Host Mismatch

GitHub Security Advisories

We recommend you create a private GitHub Security Advisory for these findings. This also allows you to invite the GHSL team to collaborate and further discuss these findings in private before they are published.

Credit

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

igrigorik commented on May 24, 2020 — Owner, Author

- Looks like this is an issue with a number of EM-powered libraries, e.g. **Security vulnerability: missing SSL hostname validation** ConradIrwin/em-imap#25
- Faraday includes an em-http patch that implements validation: lostisland/faraday@ `63cf47c`

Ideally, this should be addressed upstream in eventmachine core.. **@sodabrew** any thoughts on that? As an interim solution we could merge Faraday implementation into em-http. **@agustingianni** could you confirm that faraday implementation addresses the issue?

agustingianni commented on May 26, 2020

CVE-2020-13482 has been assigned to this issue.

Ilya, let me know when you are ready for me to test the Faraday changes and I will give it a sping.

sodabrew commented on May 26, 2020

I'd be glad to upstream that, thanks for calling it out!

igrigorik commented on May 27, 2020 — Owner, Author

@sodabrew great, I think that would be the best path forward and help resolve and prevent this same issue across a number of different libraries and services using EM.

@agustingianni in theory you should be able to test with..

```
require 'rubygems'
require 'eventmachine'
require 'em-http'

## copy local instance from https://github.com/lostisland/faraday/commit/63cf47c95b573539f047c729bd9ad67560bc83ff#diff-2ffbfc9e78f3db69aad38b56f7decad1
require 'em_http_ssl_patch.rb'


urls = ARGV
if urls.size < 1
  puts "Usage: #{$0} <url> <url> <...>"
  exit
end

pending = urls.size

EM.run do
  urls.each do |url|
    http = EM::HttpRequest.new(url).get
    http.callback {
      puts "#{url}\n#{http.response_header.status} - #{http.response.length} bytes\n"
      puts http.response

      pending -= 1
      EM.stop if pending < 1
    }
    http.errback {
      puts "#{url}\n" + http.error

      pending -= 1
      EM.stop if pending < 1
    }
  end
end
```

agustingianni commented on May 27, 2020

Fantastic, I will give it a try and will get back at you. Thank you.

agustingianni commented on May 27, 2020

So I made some changes to actually trigger the validation code, basically I added `ssl: {verify_peer: true}` to the `EM::HttpRequest` constructor. The patch seems to work fine, I have tested it both with a fake certificate that matches the host and with a valid certificate (emited for another domain) but with the DNS pointing to the target host. Both tests were successfull.

I would advice to change the default value to `verify_peer: true` but I understand that this may break some clients of the library. If thats the case, updating the documentation reflecting this important detail is a good compromise I think.

Thank you all for addressing this issue, I think this will help `em-imap` too to solve the issue. I will try to contact the author and see what we can do.

This is the client I used for testing:

```
require 'rubygems'
require 'eventmachine'
require 'em-http'

## copy local instance from https://github.com/lostisland/faraday/commit/63cf47c95b573539f047c729bd9ad67560bc83ff#diff-2ffbfc9e78f3db69aad38b56f7decad1
require './em_http_ssl_patch.rb'

urls = ARGV
if urls.size < 1
  puts "Usage: #{$0} <url> <url> <...>"
  exit
end

pending = urls.size

EM.run do
  urls.each do |url|
    http = EM::HttpRequest.new(url, ssl: {verify_peer: true}).get
    http.callback {
      puts "#{url}\n#{http.response_header.status} - #{http.response.length} bytes\n"
      puts http.response

      pending -= 1
      EM.stop if pending < 1
    }
    http.errback {
      puts "#{url}\n" + http.error

      pending -= 1
      EM.stop if pending < 1
    }
  end
end
```

agustingianni mentioned this issue on May 27, 2020

Security vulnerability: missing SSL hostname validation ConradIrwin/em-imap#25

Closed

igrigorik added a commit that referenced this issue on May 30, 2020

`Merge TLS verification patch from Faraday` ··· ✓ `7e27434`

igrigorik mentioned this issue on May 30, 2020

Merge TLS verification patch from Faraday #340

Merged

igrigorik commented on May 30, 2020 — Owner, Author

@agustingianni PR live that should, I believe, address the issue. I added an explicit warning that will get logged to STDERR if verify_peer is not set to true. Can you do another sanity check and confirm that it's working as intended, before I merge?

@sodabrew alternatively, would it make sense to merge this or similar logic into EM core?

agustingianni commented on Jun 1, 2020

Hello, yes of course. I will test it now and report back.

agustingianni commented on Jun 1, 2020

LGTM! Thank you for fixing this!

igrigorik closed this as completed in #340 on Jun 1, 2020

---

igrigorik added a commit that referenced this issue on Jun 1, 2020

`Merge TLS verification patch from Faraday (#340)` ··· ✓ `e5fa144`

igrigorik commented on Jun 1, 2020 — Owner, Author

1.1.6 should be live on rubygems now, with this merged.

Thanks again for the report and your help!

👍 1

SebouChu mentioned this issue on Jun 10, 2020

Force TLS peer verification when base URL scheme is HTTPS keenlabs/keen-gem#133

Open

aharbick mentioned this issue on Jun 14, 2020

specify verify_peer option to EM::HttpRequest oesmith/puffing-billy#293

Closed

jcoglan mentioned this issue on Jul 19, 2020

Address em-http-request warnings about `verify_peer` faye/faye#524

Closed

This was referenced on Jul 24, 2020

em-http-request CVE causing a TLS warning francois2metz/em-eventsource#18

Closed

Add "tls: {verify_peer: true}" to HttpRequest call francois2metz/em-eventsource#19

Merged

alromh87 added a commit to alromh87/em-imap that referenced this issue on Sep 13, 2020

`Fix missing SSL hostname validation [MiM Vuln]` ··· `8eac124`

alromh87 added a commit to alromh87/em-imap that referenced this issue on Sep 13, 2020

`Fix missing SSL hostname validation [MiM Vuln]` ··· `af5d7d8`

denisj added a commit to denisj/powertrack-rb that referenced this issue on Jul 23, 2021

`Fix Security vulnerability: missing SSL hostname validation` ··· `b8b0d73`

denisj mentioned this issue on Jul 23, 2021

Fix Security vulnerability: missing SSL hostname validation ecairn/powertrack-rb#7

Merged

lukaszsliwa added a commit to ably/ably-ruby that referenced this issue on Jul 28, 2021

`Enabled TLS hostname validation CVE-2020-13482 and igrigorik/em-http-…` ··· ✕ `115f7bd`

lukaszsliwa mentioned this issue on Jul 28, 2021

Enabled TLS hostname validation CVE-2020-13482 ably/ably-ruby#263

Merged

kamaradclimber added a commit to criteo/consul-templaterb that referenced this issue on Sep 2, 2021

`Validate ssl peers` ··· ✓ `c338d03`

kamaradclimber mentioned this issue on Sep 2, 2021

Validate ssl peers criteo/consul-templaterb#80

Merged

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Merge TLS verification patch from Faraday
igrigorik/em-http-request

3 participants