New issue

Jump to bottom

Security vulnerability: missing SSL hostname validation #25

Closed **ConradIrwin** opened this issue on May 18, 2020 · 5 comments

ConradIrwin commented on May 18, 2020 Owner

GitHub Security Lab (GHSL) Vulnerability Report: `GHSL-2020-095`

The GitHub Security Lab team has identified potential security vulnerabilities in em-imap.

We are committed to working with you to help resolve these issues. In this report you will find everything you need to effectively coordinate a resolution of these issues with the GHSL team.

If at any point you have concerns or questions about this process, please do not hesitate to reach out to us at `securitylab@github.com` (please include your `GHSL-2020-095`).

If you are *NOT* the correct point of contact for this report, please let us know!

Summary

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

Product

em-imap

Tested Version

v0.5

Missing SSL/TLS certificate hostname validation

em-imap 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.imap.gmail.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 993 with TLS enabled.
$ openssl s_server -key key.pem -cert cert.pem -accept 993
Using auto DH parameters
Using default temp ECDH parameters
ACCEPT
-----BEGIN SSL SESSION PARAMETERS-----
MFUCAQECAgMDBALAMAQABDB6rCbPKv6fm6PV8kaehPOpnJS6alzqvMImVDzjsSHm
ll1shwxJqlreT6XL5va01tahBgIEXsJTeqIEAgIcIKQGBAQBAAAA
-----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
```

Create a sample client with the following contents:

```
require 'rubygems'
require 'em-imap'

EM::run do
  client = EM::IMAP.new('test.imap.gmail.com', 993, true)
  client.connect.errback do |error|
    puts "Connecting failed: #{error}"
  end.callback do |hello_response|
    puts "Connecting succeeded!"
    puts hello_response
  end.bothback do
    EM::stop
  end
end
```

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

```
# Run the example client.
$ ruby em-imap-client.rb
```

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).

Contact

You can contact the GHSL team at `securitylab@github.com`, please include the `GHSL-2020-095` in any communication regarding this issue.

Disclosure Policy

This report is subject to our coordinated disclosure policy.

👍 1

agustingianni commented on May 20, 2020

CVE-2020-13163

igrigorik mentioned this issue on May 24, 2020

Security vulnerability: missing SSL hostname validation igrigorik/em-http-request#339

Closed

agustingianni commented on May 27, 2020

Hello **@ConradIrwin** we have been working with the folks from em-http-request and I think we have reached a good patch for this issue that may be usable in your library. If you decide to implement it, I would love to help you with the testing.

You can find more information in the thread at igrigorik/em-http-request#339

Thanks.

ConradIrwin commented on May 27, 2020 Owner Author

Thanks! That's great news. I'm going to check back in ~2 weeks and see whether there's a solution that has been upstreamed to eventmachine itself (as I don't think em-imap has any users, I'd rather wait and fix this properly than go through a few rounds of patches)

Sent via Superhuman (https://sprh.mn/?vip=conrad.irwin@gmail.com)
...

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

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

alromh87 commented on Sep 13, 2020 Contributor

@agustingianni Implemeted a fix based on the information you provided

Thank you

huntr-helper commented on Sep 17, 2020

🛠️ A fix has been provided for this issue. Please reference: 418sec#1

🔥 This fix has been provided through the https://huntr.dev/ bug bounty platform.

huntr-helper mentioned this issue on Sep 17, 2020

Security Fix for Man-in-the-Middle - huntr.dev #27

Merged

ConradIrwin closed this as completed in `8eac124` on Sep 18, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants