August 26, 2020

GHSL-2020-095 : Monster in the middle attack in em-imap - CVE-2020-13163

Agustin Gianni

Summary

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

Product

em-imap

Tested Version

v0.5

Details

Missing SSL/TLS certificate hostname validation

em-imap 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.

Remediation

Implement hostname validation.

References

CWE-297: Improper Validation of Certificate with Host Mismatch

CVE

CVE-2020-13163

Timeline

- 18/05/2020: Report sent to Vendor
- 18/05/2020: Vendor acknowledged report
- 19/05/2020: Report published to public

Resources

- ConradIrwin/em-imap#25

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.

- © 2021 GitHub, Inc.