skip to content
Back to GitHub.com
Security Lab
Bounties Research Advisories Get Involved Events
Home Bounties Research Advisories Get Involved Events

June 17, 2020

GHSL-2020-094: Missing SSL/TLS certificate hostname validation in em-http-request - CVE-2020-13482

Agustin Gianni

Summary

Missing hostname validation allows an attacker to perform a person in the middle attack against users of the em-http-request library.

Product

em-http-request

Tested Version

1.1.5

Details

GHSL-2020-094: Missing SSL/TLS certificate hostname validation

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

CVE

- CVE-2020-13482

Coordinated Disclosure Timeline

This report was subject to the GHSL coordinated disclosure policy.

- 18/05/2020: Report sent to Vendor
- 23/05/2020: Vendor acknowledged report
- 24/05/2020: Report published to public
- 30/05/2020: Vendor fixed the issue.

Resources

- https://cwe.mitre.org/data/definitions/297.html
- https://github.com/igrigorik/em-http-request/issues/339
- https://github.com/igrigorik/em-http-request/pull/340

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-ID: `GHSL-2020-094` in any communication regarding this issue.

GitHub

Product

- Features
- Security
- Enterprise
- Customer stories
- Pricing
- Resources

Platform

- Developer API
- Partners
- Atom
- Electron
- GitHub Desktop

Support

- Docs
- Community Forum
- Professional Services
- Status
- Contact GitHub

Company

- About
- Blog

-
-
-
-
-