



CVE-2020-13163

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-13163
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-19 22:15:00 UTC
Updated	2021-03-04 21:20:00 UTC
Description	em-imap 0.5 uses the library eventmachine in an insecure way that allows an attacker to perform a man-in-the-middle attack

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Em-imap Project	Em-imap	0.5	All	All	All
Application	Em-imap Project	Em-imap	0.5	All	All	All

References

Reference	Source	Link
Security vulnerability: missing SSL hostname validation · Issue #25 · Conradlrwin/em-imap · GitHub	MISC	github.com
GHSL-2020-095 : Monster in the middle attack in em-imap - CVE-2020-13163 - GitHub Security Lab	MISC	securitylab.github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report