net-imap vulnerable to STARTTLS stripping via invalid response timing

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-42246
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-09 20:16:28 UTC
Updated	2026-05-09 20:16:28 UTC
Description	Net::IMAP implements Internet Message Access Protocol (IMAP) client functionality in Ruby. Prior to versions 0.3.10, 0.4.2

Risk And Classification

Primary CVSS: v4.0 7.6 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-392 | CWE-393 | CWE-636 | CWE-754 | CWE-841 | CWE-392 CWE-392: Missing Report of Error Condition | CWE-393 CWE-393: Return of Wrong Status Code | CWE-754 CWE-754: Improper Check for Unusual or Exceptional Conditions | CWE-636 CWE-636: Not Failing Securely ('Failing Open') | CWE-841 CWE-841: Improper Enforcement of Behavioral Workflow

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	7.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/S
4.0	CNA	DECLARED	7.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ruby	Net-imap	affected < 0.3.10	Not specified
CNA	Ruby	Net-imap	affected >= 0.4.0, < 0.4.24	Not specified
CNA	Ruby	Net-imap	affected >= 0.5.0, < 0.5.14	Not specified
CNA	Ruby	Net-imap	affected >= 0.6.0, < 0.6.4	Not specified

References

Reference	Source	Link	Tags
github.com/ruby/net-imap/commit/24a4e770b43230286a05aa2a9746cdbb3eb8485e	security-advisories@github.com	github.com	
github.com/ruby/net-imap/releases/tag/v0.5.14	security-advisories@github.com	github.com	
github.com/ruby/net-imap/commit/f79d35bf5833f186e81044c57c843eda30c873da	security-advisories@github.com	github.com	
github.com/ruby/net-imap/commit/0ede4c40b1523dfeaf95777b2678e54cc0fd9618	security-advisories@github.com	github.com	
github.com/ruby/net-imap/releases/tag/v0.4.24	security-advisories@github.com	github.com	
github.com/ruby/net-imap/releases/tag/v0.3.10	security-advisories@github.com	github.com	
github.com/ruby/net-imap/commit/97e2488fb5401a1783bddd959dde007d9fbce42c	security-advisories@github.com	github.com	
github.com/ruby/net-imap/security/advisories/GHSA-vcgp-9326-pqcp	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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