# net-imap: Command Injection via "raw" arguments to multiple commands

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-42257 |
| **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 0.4.24, 0.5.1 |

## Risk And Classification

**Primary CVSS:** v4.0 5.8 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:P/VC:N/VI:H/VA:L/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-77 | CWE-93 | CWE-93 CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') | CWE-77 CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | security-advisories@github.com | Secondary | 5.8 | MEDIUM | CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:P/VC:N/VI:H/VA:L/SC:N/S |
| 4.0 | CNA | DECLARED | 5.8 | MEDIUM | CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:P/VC:N/VI:H/VA:L/SC:N/S |

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

High

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:P/VC:N/VI:H/VA:L/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 < 0.4.24 | 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/releases/tag/v0.6.4 | 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/security/advisories/GHSA-hm49-wcqc-g2xg | security-advisories@github.com | github.com | |
| github.com/ruby/net-imap/releases/tag/v0.4.24 | security-advisories@github.com | github.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

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**