



# net-imap: Denial of service via high iteration count for `SCRAM-\*` authentication

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

## Summary

<b>CVE</b>	CVE-2026-42256
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-09 20:16:28 UTC
<b>Updated</b>	2026-05-09 20:16:28 UTC
<b>Description</b>	Net::IMAP implements Internet Message Access Protocol (IMAP) client functionality in Ruby. From versions 0.4.0 to before

## Risk And Classification

**Primary CVSS:** v4.0 6 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:N/VA:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-770 | CWE-1322 | CWE-1322 CWE-1322: Use of Blocking Code in Single-threaded, Non-blocking Context | CWE-770 CWE-770: Allocation of Resources Without Limits or Throttling

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:N/VA:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:N/VA:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:N/VA:H/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/MSX/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 >= 0.4.0, < 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/808001bc45c06f7297a7e96d341279e041a7f7f4	security-advisories@github.com	github.com	
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/commit/99f59eab6064955a23debd95410263ad144df758	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/security/advisories/GHSA-87pf-fpww-p7m7	security-advisories@github.com	github.com	
github.com/ruby/net-imap/commit/158d0b505074397cdb5ceb58935e42dd2bcfa612	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)