mruby nregs codegen.c scope_new heap-based overflow

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

Summary

CVE	CVE-2025-7207
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-09 01:15:50 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability, which was classified as problematic, was found in mruby up to 3.4.0-rc2. Affected is the function scope_new

Risk And Classification

Primary CVSS: v4.0 1.9 LOW from cna@vuldb.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/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-119 | CWE-122 | CWE-787 | CWE-122 Heap-based Buffer Overflow | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	1.9	LOW	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	cna@vuldb.com	Secondary	3.3	LOW	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	DECLARED	3.3	LOW	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	3.3	LOW	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	1.7		AV:L/AC:L/Au:S/C:N/I:N/A:P
2.0	CNA	DECLARED	1.7		AV:L/AC:L/Au:S/C:N/I:N/A:P/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/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

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v3.0 Breakdown

Attack Vector

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mruby	Mruby	All	All	All	All
Application	Mruby	Mruby	3.4.0	rc	All	All
Application	Mruby	Mruby	3.4.0	rc2	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Mruby	affected 3.4.0-rc1	Not specified
CNA	Na	Mruby	affected 3.4.0-rc2	Not specified

References

Reference	Source	Link
github.com/mruby/mruby/issues/6509	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/user-attachments/files/19619499/mruby_crash.txt	cna@vuldb.com	github.com
vuldb.com	cna@vuldb.com	vuldb.com
vuldb.com	cna@vuldb.com	vuldb.com
github.com/mruby/mruby/commit/1fdd96104180cc0fb5d3cb086b05ab6458911bb9	cna@vuldb.com	github.com
vuldb.com	cna@vuldb.com	vuldb.com
github.com/mruby/mruby/issues/6509	cna@vuldb.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: JJLeo (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-07-07T00:00:00.000Z	Advisory disclosed
CNA	2025-07-07T02:00:00.000Z	VulDB entry created
CNA	2025-07-07T14:27:08.000Z	VulDB entry last update

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