CVE-2017-9527

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

Summary

CVE	CVE-2017-9527
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-11 17:29:00 UTC
Updated	2022-05-12 20:08:00 UTC
Description	The mark_context_stack function in gc.c in mruby through 1.2.0 allows attackers to cause a denial of service (heap-based u

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Mruby	Mruby	All	All	All	All

References

Reference	Source	Link	Tags
Clear unused stack region that may refer freed objects; fix #3596 · mruby/mruby@5c114c9 · GitHub	CONFIRM	github.com	Issue Tr
Heap use-after-free in mark_context_stack · Issue #3486 · mruby/mruby · GitHub	CONFIRM	github.com	Issue Tr
[SECURITY] [DLA 2996-1] mruby security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179269 Debian Security Update for mruby (DLA 2996-1)

© 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 registred 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