CVE-2014-4975

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

Summary

CVE	CVE-2014-4975
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-15 20:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Off-by-one error in the encodes function in pack.c in Ruby 1.9.3 and earlier, and 2.x through 2.1.2, when using certain forma

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:N/A:N

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All

Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Ruby-lang	Ruby	2.0	All	All	All
Application	Ruby-lang	Ruby	2.0.0	All	All	All
Application	Ruby-lang	Ruby	2.0.0	p0	All	All
Application	Ruby-lang	Ruby	2.0.0	p195	All	All
Application	Ruby-lang	Ruby	2.0.0	p247	All	All
Application	Ruby-lang	Ruby	2.0.0	preview1	All	All
Application	Ruby-lang	Ruby	2.0.0	preview2	All	All
Application	Ruby-lang	Ruby	2.0.0	rc1	All	All
Application	Ruby-lang	Ruby	2.0.0	rc2	All	All
Application	Ruby-lang	Ruby	2.1	-	All	All
Application	Ruby-lang	Ruby	2.1	preview1	All	All
Application	Ruby-lang	Ruby	2.1.1	All	All	All
Application	Ruby-lang	Ruby	2.1.2	All	All	All
Application	Ruby-lang	Ruby	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Red Hat Customer Portal	af854a3a-212
Bug 1118158 – CVE-2014-4975 ruby: off-by-one stack-based buffer overflow in the encodes() function	af854a3a-212
IBM X-Force Exchange	af854a3a-212
Red Hat Customer Portal	af854a3a-212
USN-2397-1: Ruby vulnerabilities | Ubuntu	af854a3a-212
Mageia Advisory: MGASA-2014-0472 - Updated ruby packages fix security vulnerabilities	af854a3a-212
Bug #10019: segmentation fault/buffer overrun in pack.c (encodes) - ruby-trunk - Ruby Issue Tracking System	af854a3a-212
Ruby 'pack.c' Buffer Overflow Vulnerability	af854a3a-212

Ruby 'pack.c' Buffer Overflow Vulnerability	af854a3a-212
Oracle Linux Bulletin - January 2016	af854a3a-212
oss-security - Fwd: [ruby-core:63604] [ruby-trunk - Bug #10019] [Open] segmentation fault/buffer overrun in pack.c (encodes)	af854a3a-212
Red Hat Customer Portal	af854a3a-212
Support / Security / Advisories / / MDVSA-2015:129 | Mandriva	af854a3a-212
[ruby] Revision 46778	af854a3a-212
Debian -- Security Information -- DSA-3157-1 ruby1.9.1	af854a3a-212
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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