CVE-2011-2705

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

Summary

CVE	CVE-2011-2705
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-08-05 21:55:04 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The SecureRandom.random_bytes function in lib/securerandom.rb in Ruby before 1.8.7-p352 and 1.9.x before 1.9.2-p290

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-20 | 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
Application	Ruby-lang	Ruby	1.8.7	p22	All	All

Application	Ruby-lang	Ruby	1.8.7	p71	All	All
Application	Ruby-lang	Ruby	1.8.7	p72	All	All
Application	Ruby-lang	Ruby	1.8.7-160	All	All	All
Application	Ruby-lang	Ruby	1.8.7-173	All	All	All
Application	Ruby-lang	Ruby	1.8.7-248	All	All	All
Application	Ruby-lang	Ruby	1.8.7-249	All	All	All
Application	Ruby-lang	Ruby	1.8.7-299	All	All	All
Application	Ruby-lang	Ruby	1.8.7-302	All	All	All
Application	Ruby-lang	Ruby	1.8.7-330	All	All	All
Application	Ruby-lang	Ruby	1.8.7-p21	All	All	All
Application	Ruby-lang	Ruby	1.9	All	All	All
Application	Ruby-lang	Ruby	1.9	r18423	All	All
Application	Ruby-lang	Ruby	1.9.0	All	All	All
Application	Ruby-lang	Ruby	1.9.0	r18423	All	All
Application	Ruby-lang	Ruby	1.9.0-0	All	All	All
Application	Ruby-lang	Ruby	1.9.0-1	All	All	All
Application	Ruby-lang	Ruby	1.9.0-2	All	All	All
Application	Ruby-lang	Ruby	1.9.0-20060415	All	All	All
Application	Ruby-lang	Ruby	1.9.0-20070709	All	All	All
Application	Ruby-lang	Ruby	1.9.1	All	All	All
Application	Ruby-lang	Ruby	1.9.1	-p0	All	All
Application	Ruby-lang	Ruby	1.9.1	-p129	All	All
Application	Ruby-lang	Ruby	1.9.1	-p243	All	All
Application	Ruby-lang	Ruby	1.9.1	-p376	All	All
Application	Ruby-lang	Ruby	1.9.1	-p429	All	All
Application	Ruby-lang	Ruby	1.9.1	-preview_1	All	All
Application	Ruby-lang	Ruby	1.9.1	-preview_2	All	All
Application	Ruby-lang	Ruby	1.9.1	-rc1	All	All
Application	Ruby-lang	Ruby	1.9.1	-rc2	All	All
Application	Ruby-lang	Ruby	1.9.2	All	All	All
Application	Ruby-lang	Ruby	1.9.2	dev	All	All
Application	Ruby-lang	Ruby	1.9.2-p136	All	All	All
Application	Ruby-lang	Ruby	1.9.2-p180	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
oss-security - CVE Request: ruby PRNG fixes
svn.ruby-lang.org/repos/ruby/tags/v1_8_7_352/ChangeLog
oss-security - Re: CVE Request: ruby PRNG fixes
oss-security - Re: CVE Request: ruby PRNG fixes
Ruby 1.8.7-p352 released
[ruby] Revision 32050
oss-security - Re: CVE Request: ruby PRNG fixes
svn.ruby-lang.org/repos/ruby/tags/v1_9_2_290/ChangeLog
[SECURITY] Fedora 15 Update: ruby-1.8.7.352-1.fc15
Ruby Random Number Generation Local Denial Of Service Vulnerability
722415 – (CVE-2011-2686, CVE-2011-2705, CVE-2011-3009) CVE-2011-2686 CVE-2011-2705 CVE-2011-3009 ruby: Properly initialize the r
[SECURITY] Fedora 14 Update: ruby-1.8.7.352-1.fc14
Support
Ruby 1.9.2-p290 is released
Bug #4579: SecureRandom + OpenSSL may repeat with fork - Ruby master - Ruby Issue Tracking System
CVE Program record
NVD vulnerability detail

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**