CVE-2009-5147

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

Summary

CVE	CVE-2009-5147
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-29 14:59:00 UTC
Updated	2018-03-28 01:29:00 UTC
Description	DL::dlopen in Ruby 1.8, 1.9.0, 1.9.2, 1.9.3, 2.0.0 before patchlevel 648, and 2.1 before 2.1.8 opens libraries with tainted nar

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ruby-lang	Ruby	1.8.0	All	All	All
Application	Ruby-lang	Ruby	1.9.0	All	All	All
Application	Ruby-lang	Ruby	1.9.2	All	All	All
Application	Ruby-lang	Ruby	1.9.3	All	All	All
Application	Ruby-lang	Ruby	2.0.0	All	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	p353	All	All
Application	Ruby-lang	Ruby	2.0.0	p481	All	All
Application	Ruby-lang	Ruby	2.0.0	p576	All	All
Application	Ruby-lang	Ruby	2.0.0	p594	All	All
Application	Ruby-lang	Ruby	2.0.0	p598	All	All
Application	Ruby-lang	Ruby	2.0.0	p643	All	All
Application	Ruby-lang	Ruby	2.0.0	p645	All	All
Application	Ruby-lang	Ruby	2.0.0	p647	All	All
Application	Ruby-lang	Ruby	2.1.0	All	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	2.1.3	All	All	All
Application	Ruby-lang	Ruby	2.1.4	All	All	All
Application	Ruby-lang	Ruby	2.1.5	All	All	All
Application	Ruby-lang	Ruby	2.1.6	All	All	All
Application	Ruby-lang	Ruby	2.1.7	All	All	All
Application	Ruby-lang	Ruby	1.8.0	All	All	All
Application	Ruby-lang	Ruby	1.9.0	All	All	All
Application	Ruby-lang	Ruby	1.9.2	All	All	All
Application	Ruby-lang	Ruby	1.9.3	All	All	All
Application	Ruby-lang	Ruby	2.0.0	All	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	p353	All	All
Application	Ruby-lang	Ruby	2.0.0	p481	All	All
Application	Ruby-lang	Ruby	2.0.0	p576	All	All
Application	Ruby-lang	Ruby	2.0.0	p594	All	All
Application	Ruby-lang	Ruby	2.0.0	p598	All	All
Application	Ruby-lang	Ruby	2.0.0	p643	All	All
Application	Ruby-lang	Ruby	2.0.0	p645	All	All
Application	Ruby-lang	Ruby	2.0.0	p647	All	All
Application	Ruby-lang	Ruby	2.1.0	All	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	2.1.3	All	All	All
Application	Ruby-lang	Ruby	2.1.4	All	All	All
Application	Ruby-lang	Ruby	2.1.5	All	All	All
Application	Ruby-lang	Ruby	2.1.6	All	All	All
Application	Ruby-lang	Ruby	2.1.7	All	All	All

References

Reference	Source	Link
oss-sec: Re: CVE request: Two ruby 'dl' vulnerabilities fixed in ruby-1.9.1-p129	MLIST	seclists.org
Bug 1248935 – CVE-2009-5147 CVE-2015-7551 ruby: DL::dlopen could open a library with tainted library name	CONFIRM	bugzilla.redha
Ruby 'dl/handle.c' Security Bypass Vulnerability	BID	www.securityf

Red Hat Customer Portal	REDHAT	access.redhat
CVE-2015-7551: Unsafe tainted string usage in Fiddle and DL	CONFIRM	www.ruby-lang
* ext/dl/dl.c (rb_dlhandle_initialize): prohibits DL::dlopen · ruby/ruby@4600cf7 · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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