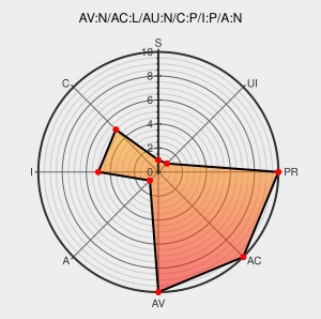
CVE-2013-2065

Published on: 11/02/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:14 AM UTC

CVE-2013-2065

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Opensuse from Opensuse contain the following vulnerability:

(1) DL and (2) Fiddle in Ruby 1.9 before 1.9.3 patchlevel 426, and 2.0 before 2.0.0 patchlevel 195, do not perform taint checking for native functions, which allows context-dependent attackers to bypass intended $SAFE level restrictions.

CVE-2013-2065 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
[SECURITY] Fedora 18 Update: ruby-1.9.3.429-30.fc18	lists.fedoraproject.org, text/html	FEDORA FEDORA-2013-8375
openSUSE-SU-2013:1611-1: moderate: update for ruby19	Vendor Advisory, lists.opensuse.org, text/html	SUSE openSUSE-SU-2013:1611
CVE-2013-2065 | Puppet	puppet.com, text/html	CONFIRM puppet.com/security/cve/cve-2013-2065
USN-2035-1: Ruby vulnerabilities | Ubuntu	www.ubuntu.com, text/html	UBUNTU USN-2035-1
Object taint bypassing in DL and Fiddle in Ruby (CVE-2013-2065)	Exploit, Patch, Vendor Advisory, www.ruby-lang.org	CONFIRM www.ruby-lang.org/en/news/2013/05/14/taint-bypass-dl-fiddle-cve-2013-2065/

	text/html	
[SECURITY] Fedora 17 Update: ruby-1.9.3.429-30.fc17	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-8411
[SECURITY] Fedora 19 Update: ruby-2.0.0.195-8.fc19	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-8738

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Application	Ruby-lang	Ruby	1.9	All	All	All
Application	Ruby-lang	Ruby	1.9.1	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	1.9.3	p0	All	All
Application	Ruby-lang	Ruby	1.9.3	p125	All	All
Application	Ruby-lang	Ruby	1.9.3	p194	All	All
Application	Ruby-lang	Ruby	1.9.3	p286	All	All
Application	Ruby-lang	Ruby	1.9.3	p383	All	All
Application	Ruby-lang	Ruby	1.9.3	p385	All	All
Application	Ruby-lang	Ruby	1.9.3	p392	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	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	1.9	All	All	All
Application	Ruby-lang	Ruby	1.9.1	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	1.9.3	p0	All	All
Application	Ruby-lang	Ruby	1.9.3	p125	All	All
Application	Ruby-lang	Ruby	1.9.3	p194	All	All
Application	Ruby-lang	Ruby	1.9.3	p286	All	All
Application	Ruby-lang	Ruby	1.9.3	p383	All	All
Application	Ruby-lang	Ruby	1.9.3	p385	All	All
Application	Ruby-lang	Ruby	1.9.3	p392	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	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

cpe:2.3:o:opensuse:opensuse:12.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9:*:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.1:*:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:*:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p0:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p125:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p194:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p286:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p383:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p385:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p392:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0.0:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0.0:p0:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0.0:preview1:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0.0:preview2:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0.0:rc1:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0.0:rc2:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.1:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.2:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p0:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p125:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p194:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p286:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p383:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p385:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.9.3:p392:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0.0:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0.0:p0:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0.0:preview1:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0.0:preview2:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0.0:rc1:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:2.0.0:rc2:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→