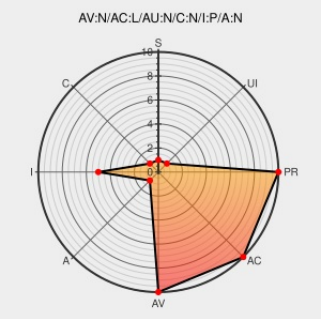
CVE-2012-4464

Published on: 04/25/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:15 PM UTC

CVE-2012-4464

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



Certain versions of Ruby from Ruby-lang contain the following vulnerability:

Ruby 1.9.3 before patchlevel 286 and 2.0 before revision r37068 allows context-dependent attackers to bypass safe-level restrictions and modify untainted strings via the (1) exc_to_s or (2) name_err_to_s API function, which marks the string as tainted, a different vulnerability than CVE-2012-4466. NOTE: this issue might exist because of a CVE-2011-1005 regression.

CVE-2012-4464 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
[SECURITY] Fedora 18 Update: ruby-1.9.3.194-18.fc18	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-15376
[ruby] Revision 37068	svn.ruby-lang.org text/html	MISC svn.ruby-lang.org/cgi-bin/viewvc.cgi?view=revision&revision=37068
oss-security - Re: CVE Request: Ruby safe level bypasses	www.openwall.com text/html	MLIST [oss-security] 20121003 Re: CVE Request: Ruby safe level bypasses
862598 – (CVE-2012-4464) CVE-2012-4464 ruby 1.9.3: Possibility to bypass Ruby's $SAFE (level 4) semantics	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=862598

oss-security - CVE Request: Ruby safe level bypasses	www.openwall.com text/html	MLIST [oss-security] 20121002 CVE Request: Ruby safe level bypasses
$SAFE escaping vulnerability about Exception#to_s / NameError#to_s (CVE-2012-4464, CVE-2012-4466)	Vendor Advisory www.ruby-lang.org text/html	CONFIRM www.ruby-lang.org/en/news/2012/10/12/cve-2012-4464-cve-2012-4466/
[SECURITY] Fedora 17 Update: ruby-1.9.3.194-17.fc17	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-15395

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	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	1.9.3	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	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: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: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:1.9.3:*:*:*:*:*:*:*:

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: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→

CVE.report and Source URL Uptime Status status.cve.report