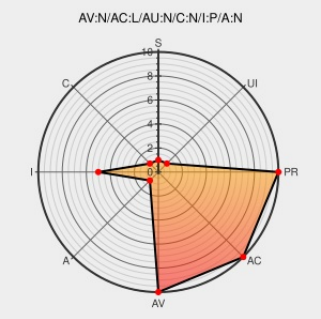
CVE-2012-4522

Published on: 11/24/2012 12:00:00 AM UTC

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

CVE-2012-4522

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



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

The rb_get_path_check function in file.c in Ruby 1.9.3 before patchlevel 286 and Ruby 2.0.0 before r37163 allows context-dependent attackers to create files in unexpected locations or with unexpected names via a NUL byte in a file path.

CVE-2012-4522 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
oss-security - CVE request: ruby file creation due in insertion of illegal NUL character	www.openwall.com text/html	MLIST [oss-security] 20121012 CVE request: ruby file creation due in insertion of illegal NUL character
[ruby] Revision 37163	svn.ruby-lang.org text/html	MISC svn.ruby-lang.org/cgi-bin/viewvc.cgi?view=revision&revision=37163
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0129
oss-security - Re: CVE request: ruby file creation due in insertion of illegal NUL character	www.openwall.com text/html	MLIST [oss-security] 20121016 Re: CVE request: ruby file creation due in insertion of illegal NUL character
[SECURITY] Fedora 18 Update: ruby-1.9.3.286-19.fc18	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-16071

[SECURITY] Fedora 17 Update: ruby-1.9.3.286-18.fc17	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-16086
Unintentional file creation caused by inserting an illegal NUL character (CVE-2012-4522)	www.ruby-lang.org text/html	CONFIRM www.ruby-lang.org/en/news/2012/10/12/poisoned-NUL-byte-vulnerability/
oss-security - Re: CVE request: ruby file creation due in insertion of illegal NUL character	www.openwall.com text/html	MLIST [oss-security] 20121013 Re: CVE request: ruby file creation due in insertion of illegal NUL character

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	2.0.0	All	All	All
Application	Ruby-lang	Ruby	1.9.3	All	All	All
Application	Ruby-lang	Ruby	2.0.0	All	All	All

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→