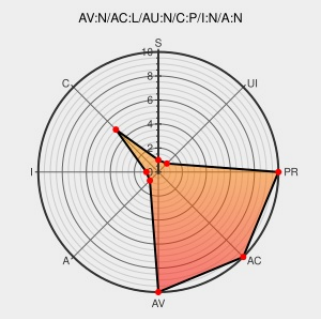
CVE-2008-1891

Published on: 04/18/2008 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:13 PM UTC

CVE-2008-1891

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



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

Directory traversal vulnerability in WEBrick in Ruby 1.8.4 and earlier, 1.8.5 before 1.8.5-p231, 1.8.6 before 1.8.6-p230, 1.8.7 before 1.8.7-p22, and 1.9.0 before 1.9.0-2, when using NTFS or FAT filesystems, allows remote attackers to read arbitrary CGI files via a trailing (1) + (plus), (2) %2b (encoded plus), (3) . (dot), (4) %2e (encoded dot), or (5) %20 (encoded space) character in the URI, possibly related to the WEBrick::HTTPServlet::FileHandler and WEBrick::HTTPServer.new functionality and the :DocumentRoot option.

CVE-2008-1891 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Fedora update for ruby - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 30831
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 31687
[security-announce] SUSE Security Summary Report SUSE-SR:2008:017	lists.opensuse.org text/html	SUSE SUSE-SR:2008:017
[SECURITY] Fedora 9 Update: ruby-1.8.6.230-1.fc9	www.redhat.com text/html	FEDORA FEDORA-2008-5649

Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2008-1245
Arbitrary code execution vulnerabilities	www.ruby-lang.org text/html	CONFIRM www.ruby-lang.org/en/news/2008/06/20/arbitrary-code-execution-vulnerabilities/
	aluigi.altervista.org text/plain	MISC aluigi.altervista.org/adv/webrickcgi-adv.txt
Support / Security / Advisories / / MDVSA-2008:141 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2008:141
Support / Security / Advisories / / MDVSA-2008:140 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2008:140
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ruby-webrick-cgi-info-disclosure(41824)
Ruby Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 29794

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	1.8.5	All	All	All
Application	Ruby-lang	Ruby	1.8.6	All	All	All
Application	Ruby-lang	Ruby	1.8.5	All	All	All
Application	Ruby-lang	Ruby	1.8.6	All	All	All
Application	Ruby-lang	Ruby	All	All	All	All

cpe:2.3:a:ruby-lang:ruby:1.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.8.6:*:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:ruby-lang:ruby:1.8.6:*:*:*:*:*:*:*:

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

← Previous ID

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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