



[MITRE](#)
[NVD](#)
[CVE.ORG](#)
[JSON API](#)
[Print: PDF](#)

CVE	CVE-2008-2664
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-06-24 19:41:00 UTC
Updated	2018-11-01 15:06:00 UTC
Description	The rb_str_format function 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-p230, 1.9.0 before 1.9.0-p230, 1.9.1 before 1.9.1-p230, 1.9.2 before 1.9.2-p230, 1.9.3 before 1.9.3-p230, 1.9.4 before 1.9.4-p230, 1.9.5 before 1.9.5-p230, 1.9.6 before 1.9.6-p230, 1.9.7 before 1.9.7-p230, 1.9.8 before 1.9.8-p230, 1.9.9 before 1.9.9-p230, 1.9.10 before 1.9.10-p230, 1.9.11 before 1.9.11-p230, 1.9.12 before 1.9.12-p230, 1.9.13 before 1.9.13-p230, 1.9.14 before 1.9.14-p230, 1.9.15 before 1.9.15-p230, 1.9.16 before 1.9.16-p230, 1.9.17 before 1.9.17-p230, 1.9.18 before 1.9.18-p230, 1.9.19 before 1.9.19-p230, 1.9.20 before 1.9.20-p230, 1.9.21 before 1.9.21-p230, 1.9.22 before 1.9.22-p230, 1.9.23 before 1.9.23-p230, 1.9.24 before 1.9.24-p230, 1.9.25 before 1.9.25-p230, 1.9.26 before 1.9.26-p230, 1.9.27 before 1.9.27-p230, 1.9.28 before 1.9.28-p230, 1.9.29 before 1.9.29-p230, 1.9.30 before 1.9.30-p230, 1.9.31 before 1.9.31-p230, 1.9.32 before 1.9.32-p230, 1.9.33 before 1.9.33-p230, 1.9.34 before 1.9.34-p230, 1.9.35 before 1.9.35-p230, 1.9.36 before 1.9.36-p230, 1.9.37 before 1.9.37-p230, 1.9.38 before 1.9.38-p230, 1.9.39 before 1.9.39-p230, 1.9.40 before 1.9.40-p230, 1.9.41 before 1.9.41-p230, 1.9.42 before 1.9.42-p230, 1.9.43 before 1.9.43-p230, 1.9.44 before 1.9.44-p230, 1.9.45 before 1.9.45-p230, 1.9.46 before 1.9.46-p230, 1.9.47 before 1.9.47-p230, 1.9.48 before 1.9.48-p230, 1.9.49 before 1.9.49-p230, 1.9.50 before 1.9.50-p230, 1.9.51 before 1.9.51-p230, 1.9.52 before 1.9.52-p230, 1.9.53 before 1.9.53-p230, 1.9.54 before 1.9.54-p230, 1.9.55 before 1.9.55-p230, 1.9.56 before 1.9.56-p230, 1.9.57 before 1.9.57-p230, 1.9.58 before 1.9.58-p230, 1.9.59 before 1.9.59-p230, 1.9.60 before 1.9.60-p230, 1.9.61 before 1.9.61-p230, 1.9.62 before 1.9.62-p230, 1.9.63 before 1.9.63-p230, 1.9.64 before 1.9.64-p230, 1.9.65 before 1.9.65-p230, 1.9.66 before 1.9.66-p230, 1.9.67 before 1.9.67-p230, 1.9.68 before 1.9.68-p230, 1.9.69 before 1.9.69-p230, 1.9.70 before 1.9.70-p230, 1.9.71 before 1.9.71-p230, 1.9.72 before 1.9.72-p230, 1.9.73 before 1.9.73-p230, 1.9.74 before 1.9.74-p230, 1.9.75 before 1.9.75-p230, 1.9.76 before 1.9.76-p230, 1.9.77 before 1.9.77-p230, 1.9.78 before 1.9.78-p230, 1.9.79 before 1.9.79-p230, 1.9.80 before 1.9.80-p230, 1.9.81 before 1.9.81-p230, 1.9.82 before 1.9.82-p230, 1.9.83 before 1.9.83-p230, 1.9.84 before 1.9.84-p230, 1.9.85 before 1.9.85-p230, 1.9.86 before 1.9.86-p230, 1.9.87 before 1.9.87-p230, 1.9.88 before 1.9.88-p230, 1.9.89 before 1.9.89-p230, 1.9.90 before 1.9.90-p230, 1.9.91 before 1.9.91-p230, 1.9.92 before 1.9.92-p230, 1.9.93 before 1.9.93-p230, 1.9.94 before 1.9.94-p230, 1.9.95 before 1.9.95-p230, 1.9.96 before 1.9.96-p230, 1.9.97 before 1.9.97-p230, 1.9.98 before 1.9.98-p230, 1.9.99 before 1.9.99-p230, 1.9.100 before 1.9.100-p230, 1.9.101 before 1.9.101-p230, 1.9.102 before 1.9.102-p230, 1.9.103 before 1.9.103-p230, 1.9.104 before 1.9.104-p230, 1.9.105 before 1.9.105-p230, 1.9.106 before 1.9.106-p230, 1.9.107 before 1.9.107-p230, 1.9.108 before 1.9.108-p230, 1.9.109 before 1.9.109-p230, 1.9.110 before 1.9.110-p230, 1.9.111 before 1.9.111-p230, 1.9.112 before 1.9.112-p230, 1.9.113 before 1.9.113-p230, 1.9.114 before 1.9.114-p230, 1.9.115 before 1.9.115-p230, 1.9.116 before 1.9.116-p230, 1.9.117 before 1.9.117-p230, 1.9.118 before 1.9.118-p230, 1.9.119 before 1.9.119-p230, 1.9.120 before 1.9.120-p230, 1.9.121 before 1.9.121-p230, 1.9.122 before 1.9.122-p230, 1.9.123 before 1.9.123-p230, 1.9.124 before 1.9.124-p230, 1.9.125 before 1.9.125-p230, 1.9.126 before 1.9.126-p230, 1.9.127 before 1.9.127-p230, 1.9.128 before 1.9.128-p230, 1.9.129 before 1.9.129-p230, 1.9.130 before 1.9.130-p230, 1.9.131 before 1.9.131-p230, 1.9.132 before 1.9.132-p230, 1.9.133 before 1.9.133-p230, 1.9.134 before 1.9.134-p230, 1.9.135 before 1.9.135-p230, 1.9.136 before 1.9.136-p230, 1.9.137 before 1.9.137-p230, 1.9.138 before 1.9.138-p230, 1.9.139 before 1.9.139-p230, 1.9.140 before 1.9.140-p230, 1.9.141 before 1.9.141-p230, 1.9.142 before 1.9.142-p230, 1.9.143 before 1.9.143-p230, 1.9.144 before 1.9.144-p230, 1.9.145 before 1.9.145-p230, 1.9.146 before 1.9.146-p230, 1.9.147 before 1.9.147-p230, 1.9.148 before 1.9.148-p230, 1.9.149 before 1.9.149-p230, 1.9.150 before 1.9.150-p230, 1.9.151 before 1.9.151-p230, 1.9.152 before 1.9.152-p230, 1.9.153 before 1.9.153-p230, 1.9.154 before 1.9.154-p230, 1.9.155 before 1.9.155-p230, 1.9.156 before 1.9.156-p230, 1.9.157 before 1.9.157-p230, 1.9.158 before 1.9.158-p230, 1.9.159 before 1.9.159-p230, 1.9.160 before 1.9.160-p230, 1.9.161 before 1.9.161-p230, 1.9.162 before 1.9.162-p230, 1.9.163 before 1.9.163-p230, 1.9.164 before 1.9.164-p230, 1.9.165 before 1.9.165-p230, 1.9.166 before 1.9.166-p230, 1.9.167 before 1.9.167-p230, 1.9.168 before 1.9.168-p230, 1.9.169 before 1.9.169-p230, 1.9.170 before 1.9.170-p230, 1.9.171 before 1.9.171-p230, 1.9.172 before 1.9.172-p230, 1.9.173 before 1.9.173-p230, 1.9.174 before 1.9.174-p230, 1.9.175 before 1.9.175-p230, 1.9.176 before 1.9.176-p230, 1.9.177 before 1.9.177-p230, 1.9.178 before 1.9.178-p230, 1.9.179 before 1.9.179-p230, 1.9.180 before 1.9.180-p230, 1.9.181 before 1.9.181-p230, 1.9.182 before 1.9.182-p230, 1.9.183 before 1.9.183-p230, 1

Problem Types: CWE-399

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Canonical	Ubuntu Linux	7.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Canonical	Ubuntu Linux	7.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Application	Ruby-lang	Ruby	All	All	All	All
Application	Ruby-lang	Ruby	All	All	All	All
Application	Ruby-lang	Ruby	All	All	All	All

Reference	Source
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE

www.matasano.com/log/1070/updates-on-drew-yaos-terrible-ruby-vulnerabilities	MISC
About the security content of Security Update 2008-004 and Mac OS X 10.5.4	CONFIRM
Fedora update for ruby - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
USN-621-1: Ruby vulnerabilities Ubuntu	UBUNTU
Slackware update for ruby - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Repository / Oval Repository	OVAL
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Red Hat update for ruby - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
[security-announce] SUSE Security Summary Report SUSE-SR:2008:017	SUSE
Ruby 1.8.6-p230/1.8.7 broke your app? Ruby Enterprise Edition to the rescue! « Phusion Corporate Blog	MISC
SecurityFocus	BUGTRAQ
Riding Rails: Multiple Ruby security vulnerabilities	MISC
June 2008 Ruby Security Advisory: A Summary	MISC
[SECURITY] Fedora 9 Update: ruby-1.8.6.230-1.fc9	FEDORA
APPLE-SA-2008-06-30 Security Update 2008-004 and Mac OS X v10.5.4	APPLE
ZSFA -- The Big Ruby Vulnerabilities	MISC
Support	REDHAT
issues.rpath.com/browse/RPL-2626	CONFIRM
Debian -- Security Information -- DSA-1612-1 ruby1.8	DEBIAN
About Secunia Research Flexera	SECUNIA
IBM X-Force Exchange	XF
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Ruby Bugs Let Users Deny Service and Execute Arbitrary Code - SecurityTracker	SECTRACK
Arbitrary code execution vulnerabilities	CONFIRM
Ubuntu update for ruby1.8 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Debian update for ruby1.8 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Support / Security / Advisories // MDVSA-2008:142 Mandriva	MANDRIVA
Support / Security / Advisories // MDVSA-2008:141 Mandriva	MANDRIVA
Support / Security / Advisories // MDVSA-2008:140 Mandriva	MANDRIVA
Debian -- Security Information -- DSA-1618-1 ruby1.9	DEBIAN
wiki.rpath.com/wiki/Advisories:rPSA-2008-0206	CONFIRM
Webmail - OVH	VUPEN
Ruby: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO
Ruby Multiple Array and String Handling Functions Multiple Arbitrary Code Execution Vulnerabilities	BID
rPath update for ruby - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Ruby Multiple Array and String Handling Functions Multiple Arbitrary Code Execution Vulnerabilities	SECUNIA

Debian update for ruby1.9 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Ruby 1.9.0/1.8.7/1.8.6/1.8.5 new releases (Security Fix) - Ruby - Ruby-Forum	MISC
Red Hat update for ruby - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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 registered 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)