



# CVE-2013-0262

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2013-0262
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2013-02-08 20:55:00 UTC
<b>Updated</b>	2023-02-13 04:40:00 UTC
<b>Description</b>	rack/file.rb (Rack::File) in Rack 1.5.x before 1.5.2 and 1.4.x before 1.4.5 allows attackers to access arbitrary files outside the

## Risk And Classification

### Problem Types: CWE-22

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.4.0	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.4.1	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.4.2	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.4.3	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.4.4	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.5.0	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.5.1	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.4.0	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.4.1	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.4.2	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.4.3	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.4.4	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.5.0	All	All	All
Application	<a href="#">Rack Project</a>	<a href="#">Rack</a>	1.5.1	All	All	All

## References

Reference	Source	Link	Tag
-----------	--------	------	-----

rack/file.rb at master · rack/rack · GitHub	MISC	<a href="https://github.com">github.com</a>	
CVE-2013-0262 harness.rb · GitHub	MISC	<a href="https://gist.github.com">gist.github.com</a>	
Rack: a Ruby Webserver Interface	CONFIRM	<a href="https://rack.github.com">rack.github.com</a>	
Redirecting to Google Groups	MISC	<a href="https://groups.google.com">groups.google.com</a>	
openSUSE-SU-2013:0462-1: moderate: RubyOnRails: security version update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
Google Groups	CONFIRM	<a href="https://groups.google.com">groups.google.com</a>	
Security Advisory SA52033 - Rack Insecure File Access Security Issue - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Ven
909072 – (CVE-2013-0262) CVE-2013-0262 rubygem-rack: Path sanitization information disclosure	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
Prevent symlink path traversals · rack/rack@6f237e4 · GitHub	CONFIRM	<a href="https://github.com">github.com</a>	
Google Groups	CONFIRM	<a href="https://groups.google.com">groups.google.com</a>	
909071 – (CVE-2013-0263) CVE-2013-0263 rubygem-rack: Timing attack in cookie sessions	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
Redirecting to Google Groups	MISC	<a href="https://groups.google.com">groups.google.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canc
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canc

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)