

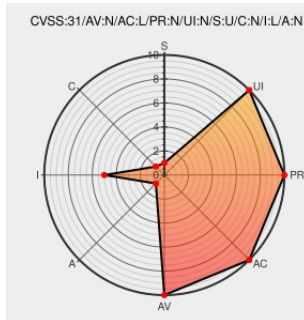


CVE-2011-3624

Published on: 11/25/2019 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:13:16 AM UTC

CVE-2011-3624

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ruby](#) from [Ruby-lang](#) contain the following vulnerability:

Various methods in WEBrick::HTTPRequest in Ruby 1.9.2 and 1.8.7 and earlier do not validate the X-Forwarded-For, X-Forwarded-Host and X-Forwarded-Server headers in requests, which might allow remote attackers to inject arbitrary text into log files or bypass intended address parsing via a crafted header.

CVE-2011-3624 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Ruby** - Ruby version = 1.9.2

Affected Vendor/Software: **Ruby** - Ruby version = 1.8.7 and earlier

CVSS3 Score: **5.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	LOW	NONE

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Taas	Link
-------------	------	------

CVE-2011-3624	Third Party Advisory security-tracker.debian.org text/html	 MISC security-tracker.debian.org/tracker/CVE-2011-3624
Ruby 1.9 - Bug #5418: Some properties of WEBrick::HTTPRequest could be malformed - Ruby Issue Tracking System	redmine.ruby-lang.org text/html	 MISC redmine.ruby-lang.org/issues/5418
CVE-2011-3624 - Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 MISC access.redhat.com/security/cve/cve-2011-3624
745636 – (CVE-2011-3624) CVE-2011-3624 Ruby WEBrick::HTTPRequest X-Forwarded-* allows arbitrary data	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-3624

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	1.8.7	All	All	All
Application	Ruby-lang	Ruby	1.9.2	All	All	All
Application	Ruby-lang	Ruby	1.8.7	All	All	All
Application	Ruby-lang	Ruby	1.9.2	All	All	All

cpe:2.3:a:ruby-lang:ruby:1.8.7:*****:

cpe:2.3:a:ruby-lang:ruby:1.9.2:*****:

cpe:2.3:a:ruby-lang:ruby:1.8.7:*****:

cpe:2.3:a:ruby-lang:ruby:1.9.2:*****:

No vendor comments have been submitted for this CVE

[← 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 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](#).

