

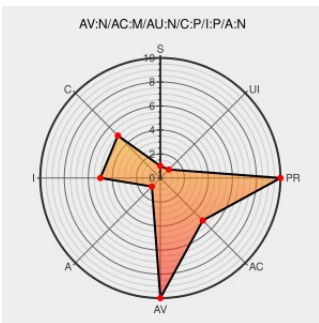


CVE-2012-2125

Published on: 10/01/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:27 PM UTC

CVE-2012-2125

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

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

RubyGems before 1.8.23 can redirect HTTPS connections to HTTP, which makes it easier for remote attackers to observe or modify a gem during installation via a man-in-the-middle attack.

CVE-2012-2125 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5.8 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

NONE

CVE References

Description

Tags

Link

Red Hat Customer Portal

[Vendor Advisory](#)

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[REDHAT RHSA-2013:1203](#)

814718 – (CVE-2012-2125, CVE-2012-2126) CVE-2012-2125 CVE-2012-2126 rubygems: Two security fixes in v1.8.23

[Patch](#)

[bugzilla.redhat.com](#)

[text/html](#)

[MISC bugzilla.redhat.com/show_bug.cgi?id=814718](#)

oss-security - Re: CVE Request -- rubygems: Two security fixes in upstream v1.8.23 version

[Patch](#)

[www.openwall.com](#)

[text/html](#)

[MLIST \[oss-security\] 20120420 Re: CVE Request -- rubygems: Two security fixes in upstream v1.8.23 version](#)

Red Hat Customer Portal

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[REDHAT RHSA-2013:1852](#)

USN-1582-1: RubyGems vulnerabilities Ubuntu	Vendor Advisory www.ubuntu.com text/html	 UBUNTU USN-1582-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2013:1441
rubygems/History.txt at 1.8 · rubygems/rubygems · GitHub	github.com text/html	 CONFIRM github.com/rubygems/rubygems/blob/1.8/History.txt
Security Advisory SA55381 - Red Hat update for rubygems - Secunia	web.archive.org text/html	 SECUNIA 55381

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
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Application	Redhat	Openshift	1.2.2	-	enterprise	All
Application	Redhat	Openshift	1.2.2	-	enterprise	All
Application	Rubygems	Rubygems	1.8.0	All	All	All
Application	Rubygems	Rubygems	1.8.1	All	All	All
Application	Rubygems	Rubygems	1.8.10	All	All	All
Application	Rubygems	Rubygems	1.8.11	All	All	All
Application	Rubygems	Rubygems	1.8.12	All	All	All
Application	Rubygems	Rubygems	1.8.13	All	All	All
Application	Rubygems	Rubygems	1.8.14	All	All	All
Application	Rubygems	Rubygems	1.8.15	All	All	All
Application	Rubygems	Rubygems	1.8.16	All	All	All
Application	Rubygems	Rubygems	1.8.17	All	All	All
Application	Rubygems	Rubygems	1.8.18	All	All	All
Application	Rubygems	Rubygems	1.8.19	All	All	All
Application	Rubygems	Rubygems	1.8.2	All	All	All
Application	Rubygems	Rubygems	1.8.20	All	All	All
Application	Rubygems	Rubygems	1.8.21	All	All	All

Application	Rubygems	Rubygems	1.8.3	All	All	All
Application	Rubygems	Rubygems	1.8.4	All	All	All
Application	Rubygems	Rubygems	1.8.5	All	All	All
Application	Rubygems	Rubygems	1.8.6	All	All	All
Application	Rubygems	Rubygems	1.8.7	All	All	All
Application	Rubygems	Rubygems	1.8.8	All	All	All
Application	Rubygems	Rubygems	1.8.9	All	All	All
Application	Rubygems	Rubygems	1.8.0	All	All	All
Application	Rubygems	Rubygems	1.8.1	All	All	All
Application	Rubygems	Rubygems	1.8.10	All	All	All
Application	Rubygems	Rubygems	1.8.11	All	All	All
Application	Rubygems	Rubygems	1.8.12	All	All	All
Application	Rubygems	Rubygems	1.8.13	All	All	All
Application	Rubygems	Rubygems	1.8.14	All	All	All
Application	Rubygems	Rubygems	1.8.15	All	All	All
Application	Rubygems	Rubygems	1.8.16	All	All	All
Application	Rubygems	Rubygems	1.8.17	All	All	All
Application	Rubygems	Rubygems	1.8.18	All	All	All
Application	Rubygems	Rubygems	1.8.19	All	All	All
Application	Rubygems	Rubygems	1.8.2	All	All	All
Application	Rubygems	Rubygems	1.8.20	All	All	All
Application	Rubygems	Rubygems	1.8.21	All	All	All
Application	Rubygems	Rubygems	1.8.3	All	All	All
Application	Rubygems	Rubygems	1.8.4	All	All	All
Application	Rubygems	Rubygems	1.8.5	All	All	All
Application	Rubygems	Rubygems	1.8.6	All	All	All
Application	Rubygems	Rubygems	1.8.7	All	All	All
Application	Rubygems	Rubygems	1.8.8	All	All	All
Application	Rubygems	Rubygems	1.8.9	All	All	All
Application	Rubygems	Rubygems	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:						
cpe:2.3:a:redhat:openshift:1.2.2:-:enterprise:*:*:*:*:						
cpe:2.3:a:redhat:openshift:1.2.2:-:enterprise:*:*:*:*:						
cpe:2.3:a:rubygems:rubygems:1.8.0:*:*:*:*:*:						

cpe:2.3:a:rubygems:rubygems:1.8.0:*****:
cpe:2.3:a:rubygems:rubygems:1.8.1:*****:
cpe:2.3:a:rubygems:rubygems:1.8.10:*****:
cpe:2.3:a:rubygems:rubygems:1.8.11:*****:
cpe:2.3:a:rubygems:rubygems:1.8.12:*****:
cpe:2.3:a:rubygems:rubygems:1.8.13:*****:
cpe:2.3:a:rubygems:rubygems:1.8.14:*****:
cpe:2.3:a:rubygems:rubygems:1.8.15:*****:
cpe:2.3:a:rubygems:rubygems:1.8.16:*****:
cpe:2.3:a:rubygems:rubygems:1.8.17:*****:
cpe:2.3:a:rubygems:rubygems:1.8.18:*****:
cpe:2.3:a:rubygems:rubygems:1.8.19:*****:
cpe:2.3:a:rubygems:rubygems:1.8.2:*****:
cpe:2.3:a:rubygems:rubygems:1.8.20:*****:
cpe:2.3:a:rubygems:rubygems:1.8.21:*****:
cpe:2.3:a:rubygems:rubygems:1.8.3:*****:
cpe:2.3:a:rubygems:rubygems:1.8.4:*****:
cpe:2.3:a:rubygems:rubygems:1.8.5:*****:
cpe:2.3:a:rubygems:rubygems:1.8.6:*****:
cpe:2.3:a:rubygems:rubygems:1.8.7:*****:
cpe:2.3:a:rubygems:rubygems:1.8.8:*****:
cpe:2.3:a:rubygems:rubygems:1.8.9:*****:
cpe:2.3:a:rubygems:rubygems:1.8.0:*****:
cpe:2.3:a:rubygems:rubygems:1.8.1:*****:
cpe:2.3:a:rubygems:rubygems:1.8.10:*****:
cpe:2.3:a:rubygems:rubygems:1.8.11:*****:
cpe:2.3:a:rubygems:rubygems:1.8.12:*****:
cpe:2.3:a:rubygems:rubygems:1.8.13:*****:
cpe:2.3:a:rubygems:rubygems:1.8.14:*****:

cpe:2.3:a:rubygems:rubygems:1.8.15:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.16:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.17:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.18:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.19:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.2:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.20:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.21:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.3:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.4:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.5:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.6:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.7:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.8:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:1.8.9:*****.*.*.*
cpe:2.3:a:rubygems:rubygems:*:*:*:*:*.*.*.*

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](#).

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