



# CVE-2015-4020

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

## Summary

<b>CVE</b>	CVE-2015-4020
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-08-25 17:59:00 UTC
<b>Updated</b>	2017-12-09 02:29:00 UTC
<b>Description</b>	RubyGems 2.0.x before 2.0.17, 2.2.x before 2.2.5, and 2.4.x before 2.4.8 does not validate the hostname when fetching ge

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Application	Rubygems	Rubygems	2.0.0	All	All	All
Application	Rubygems	Rubygems	2.0.0	preview2	All	All
Application	Rubygems	Rubygems	2.0.0	preview2.1	All	All
Application	Rubygems	Rubygems	2.0.0	preview2.2	All	All
Application	Rubygems	Rubygems	2.0.0	rc1	All	All
Application	Rubygems	Rubygems	2.0.0	rc2	All	All
Application	Rubygems	Rubygems	2.0.1	All	All	All
Application	Rubygems	Rubygems	2.0.10	All	All	All
Application	Rubygems	Rubygems	2.0.11	All	All	All
Application	Rubygems	Rubygems	2.0.12	All	All	All
Application	Rubygems	Rubygems	2.0.13	All	All	All
Application	Rubygems	Rubygems	2.0.14	All	All	All
Application	Rubygems	Rubygems	2.0.15	All	All	All
Application	Rubygems	Rubygems	2.0.16	All	All	All
Application	Rubygems	Rubygems	2.0.2	All	All	All

Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.3	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.4	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.5	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.6	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.7	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.8	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.9	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.2.0	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.2.1	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.2.2	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.2.3	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.2.4	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.0	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.1	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.2	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.3	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.4	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.5	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.6	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.7	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.0	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.0	preview2	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.0	preview2.1	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.0	preview2.2	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.0	rc1	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.0	rc2	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.1	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.10	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.11	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.12	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.13	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.14	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.15	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.16	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.2	All	All	All

Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.3	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.4	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.5	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.6	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.7	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.8	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.0.9	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.2.0	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.2.1	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.2.2	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.2.3	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.2.4	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.0	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.1	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.2	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.3	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.4	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.5	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.6	All	All	All
Application	<a href="#">Rubygems</a>	<a href="#">Rubygems</a>	2.4.7	All	All	All

## References

Reference	Source	Link	Tags
Attacking Ruby Gem Security with CVE-2015-3900	MISC	<a href="http://www.trustwave.com">www.trustwave.com</a>	Third Par
Fix API endpoint domain clamping · rubygems/rubygems@5c7bfb5 · GitHub	CONFIRM	<a href="https://github.com">github.com</a>	
Oracle Solaris Third Party Bulletin - October 2015	CONFIRM	<a href="http://www.oracle.com">www.oracle.com</a>	Third Par
2.4.8 Released   RubyGems.org	CONFIRM	<a href="http://blog.rubygems.org">blog.rubygems.org</a>	Vendor A
<a href="http://www.trustwave.com/Resources/Security-Advisories/Advisories/TWSSL2015-009">www.trustwave.com/Resources/Security-Advisories/Advisories/TWSSL2015-009</a>	MISC	<a href="http://www.trustwave.com">www.trustwave.com</a>	Third Par
2.2.5 Released   RubyGems.org	CONFIRM	<a href="http://blog.rubygems.org">blog.rubygems.org</a>	Vendor A
RubyGems CVE-2015-4020 Incomplete Fix Security Bypass Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
CVE-2015-3900, CVE-2015-4020 - Request Hijacking Vulnerability in RubyGems   Puppet	CONFIRM	<a href="http://puppet.com">puppet.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical

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](#).

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