



CVE-2020-36327

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

Summary

CVE	CVE-2020-36327
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-29 03:15:00 UTC
Updated	2023-11-07 03:22:00 UTC
Description	Bundler 1.16.0 through 2.2.9 and 2.2.11 through 2.2.16 sometimes chooses a dependency source based on the highest ge

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bundler	Bundler	All	All	All	All
Application	Bundler	Bundler	All	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Microsoft	Package Manager Configurations	-	All	All	All

References

Reference	Source	Link
Global vs block gem server source priority doesn't work as expected · Issue #3982 · rubygems/rubygems · GitHub	MISC	github.com
[SECURITY] Fedora 34 Update: ruby-3.0.2-149.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
RubyGems dependency confusion attack side of things - Running with Ruby	MISC	mensfeld.pl
Bundler: A more secure bundler: We fixed our source priorities.	MISC	bundler.io
Bundler is Still Vulnerable to Dependency Confusion Attacks (CVE-2020-36327) zofrex.com	MISC	www.zofrex.com
[SECURITY] Fedora 34 Update: ruby-3.0.2-149.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Security Update Guide - Microsoft Security Response Center	MISC	msrc.microsoft.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159326](#) Oracle Enterprise Linux Security Update for ruby:2.7 (ELSA-2021-3020)

[159635](#) Oracle Enterprise Linux Security Update for ruby:2.6 (ELSA-2022-0543)

[159636](#) Oracle Enterprise Linux Security Update for ruby:2.5 (ELSA-2022-0545)

[239536](#) Red Hat Update for ruby:2.7 (RHSA-2021:3020)

[239644](#) Red Hat Update for rh-ruby27-ruby (RHSA-2021:3559)

[239651](#) Red Hat Update for rh-ruby27-ruby (RHSA-2021:3559)

[239736](#) Red Hat Update for rh-ruby30-ruby (RHSA-2021:3982)

[240086](#) Red Hat Update for ruby:2.5 (RHSA-2022:0545)

[240088](#) Red Hat Update for ruby:2.5 (RHSA-2022:0547)

[240090](#) Red Hat Update for ruby:2.6 (RHSA-2022:0544)

[240091](#) Red Hat Update for ruby:2.5 (RHSA-2022:0546)

[240092](#) Red Hat Update for ruby:2.6 (RHSA-2022:0543)

[240116](#) Red Hat Update for rh-ruby26-ruby security (RHSA-2022:0708)

[240156](#) Red Hat Update for ruby:2.6 (RHSA-2022:0582)

[240422](#) Red Hat Update for ruby:2.5 (RHSA-2022:0548)

[281749](#) Fedora Security Update for ruby (FEDORA-2021-36cdab1f8d)

[377094](#) Alibaba Cloud Linux Security Update for ruby:2.7 (ALINUX3-SA-2021:0054)

[940383](#) AlmaLinux Security Update for ruby:2.7 (ALSA-2021:3020)

[940455](#) AlmaLinux Security Update for ruby:2.6 (ALSA-2022:0543)

[940456](#) AlmaLinux Security Update for ruby:2.5 (ALSA-2022:0545)

[960315](#) Rocky Linux Security Update for ruby:2.7 (RLSA-2021:3020)

[960771](#) Rocky Linux Security Update for ruby:2.5 (RLSA-2022:0545)

[960814](#) Rocky Linux Security Update for ruby:2.6 (RLSA-2022:0543)

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](#)