



CVE-2021-43809

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-43809
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-08 19:15:00 UTC
Updated	2023-11-16 03:04:00 UTC
Description	`Bundler` is a package for managing application dependencies in Ruby. In `bundler` versions before 2.2.33, when working v

Risk And Classification

Problem Types: CWE-88

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bundler	Bundler	All	All	All	All

References

Reference

- Securing Developer Tools: Package Managers | Sonar
- Local Code Execution through Argument Injection via dash leading git url parameter in Gemfile · Advisory · rubygems/rubygems · GitHub
- Pass "--" to git commands to separate positional and optional args by deivid-rodriguez · Pull Request #5142 · rubygems/rubygems · GitHub
- Add require parameter to `bundle add` · rubygems/rubygems@a4f2f8a · GitHub
- Changelog for Bundler version 2.2.33 · rubygems/rubygems@0fad1cc · GitHub
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[184005](#) Debian Security Update for rubygems (CVE-2021-43809)

[502023](#) Alpine Linux Security Update for ruby-bundler

© [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](#)