



CVE-2013-1656

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

Summary

CVE	CVE-2013-1656
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-03-08 18:55:00 UTC
Updated	2020-12-04 21:02:00 UTC
Description	Spree Commerce 1.0.x through 1.3.2 allows remote authenticated administrators to instantiate arbitrary Ruby objects and e

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Spreecommerce	Spree	1.0.0	All	All	All
Application	Spreecommerce	Spree	1.0.1	All	All	All
Application	Spreecommerce	Spree	1.0.2	All	All	All
Application	Spreecommerce	Spree	1.0.3	All	All	All
Application	Spreecommerce	Spree	1.0.4	All	All	All
Application	Spreecommerce	Spree	1.0.5	All	All	All
Application	Spreecommerce	Spree	1.0.6	All	All	All
Application	Spreecommerce	Spree	1.0.7	All	All	All
Application	Spreecommerce	Spree	1.1.0	All	All	All
Application	Spreecommerce	Spree	1.1.1	All	All	All
Application	Spreecommerce	Spree	1.1.2	All	All	All
Application	Spreecommerce	Spree	1.1.3	All	All	All
Application	Spreecommerce	Spree	1.1.4	All	All	All
Application	Spreecommerce	Spree	1.1.5	All	All	All
Application	Spreecommerce	Spree	1.1.6	All	All	All
Application	Spreecommerce	Spree	1.2.0	All	All	All
Application	Spreecommerce	Spree	1.2.1	All	All	All

Application	Spreecommerce	Spree	1.2.2	All	All	All
Application	Spreecommerce	Spree	1.2.3	All	All	All
Application	Spreecommerce	Spree	1.2.4	All	All	All
Application	Spreecommerce	Spree	1.3.0	All	All	All
Application	Spreecommerce	Spree	1.3.1	All	All	All
Application	Spreecommerce	Spree	1.0.0	All	All	All
Application	Spreecommerce	Spree	1.0.1	All	All	All
Application	Spreecommerce	Spree	1.0.2	All	All	All
Application	Spreecommerce	Spree	1.0.3	All	All	All
Application	Spreecommerce	Spree	1.0.4	All	All	All
Application	Spreecommerce	Spree	1.0.5	All	All	All
Application	Spreecommerce	Spree	1.0.6	All	All	All
Application	Spreecommerce	Spree	1.0.7	All	All	All
Application	Spreecommerce	Spree	1.1.0	All	All	All
Application	Spreecommerce	Spree	1.1.1	All	All	All
Application	Spreecommerce	Spree	1.1.2	All	All	All
Application	Spreecommerce	Spree	1.1.3	All	All	All
Application	Spreecommerce	Spree	1.1.4	All	All	All
Application	Spreecommerce	Spree	1.1.5	All	All	All
Application	Spreecommerce	Spree	1.1.6	All	All	All
Application	Spreecommerce	Spree	1.2.0	All	All	All
Application	Spreecommerce	Spree	1.2.1	All	All	All
Application	Spreecommerce	Spree	1.2.2	All	All	All
Application	Spreecommerce	Spree	1.2.3	All	All	All
Application	Spreecommerce	Spree	1.2.4	All	All	All
Application	Spreecommerce	Spree	1.3.0	All	All	All
Application	Spreecommerce	Spree	1.3.1	All	All	All
Application	Spreecommerce	Spree	All	All	All	All

References						
Reference					Source	Link
Conviso Application Security: Spree Commerce Multiple Unsafe Reflection Vulnerabilities (CVE-2013-1656)					MISC	blog.conviso.com.l
Not Found					MISC	www.conviso.com.
Multiple Security Vulnerabilities Fixed Spree Commerce					CONFIRM	spreecommerce.cc
CVE Program record					CVE.ORG	www.cve.org

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](#).

Free CVE JSON API [cve.report/api](#)

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