



CVE-2013-0233

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

Summary

CVE	CVE-2013-0233
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-04-25 23:55:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	Devise gem 2.2.x before 2.2.3, 2.1.x before 2.1.3, 2.0.x before 2.0.5, and 1.5.x before 1.5.4 for Ruby, when using certain de

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opsuse	Opsuse	12.2	All	All	All
Operating System	Opsuse	Opsuse	12.2	All	All	All
Application	Plataformatec	Devise	1.5.0	All	All	All
Application	Plataformatec	Devise	1.5.1	All	All	All
Application	Plataformatec	Devise	1.5.2	All	All	All
Application	Plataformatec	Devise	1.5.3	All	All	All
Application	Plataformatec	Devise	2.0.0	All	All	All
Application	Plataformatec	Devise	2.0.1	All	All	All
Application	Plataformatec	Devise	2.0.2	All	All	All
Application	Plataformatec	Devise	2.0.3	All	All	All
Application	Plataformatec	Devise	2.0.4	All	All	All
Application	Plataformatec	Devise	2.1.0	All	All	All
Application	Plataformatec	Devise	2.1.1	All	All	All
Application	Plataformatec	Devise	2.1.2	All	All	All
Application	Plataformatec	Devise	2.2.0	All	All	All
Application	Plataformatec	Devise	2.2.1	All	All	All
Application	Plataformatec	Devise	2.2.2	All	All	All

Application	Plataformatec	Devise	1.5.0	All	All	All
Application	Plataformatec	Devise	1.5.1	All	All	All
Application	Plataformatec	Devise	1.5.2	All	All	All
Application	Plataformatec	Devise	1.5.3	All	All	All
Application	Plataformatec	Devise	2.0.0	All	All	All
Application	Plataformatec	Devise	2.0.1	All	All	All
Application	Plataformatec	Devise	2.0.2	All	All	All
Application	Plataformatec	Devise	2.0.3	All	All	All
Application	Plataformatec	Devise	2.0.4	All	All	All
Application	Plataformatec	Devise	2.1.0	All	All	All
Application	Plataformatec	Devise	2.1.1	All	All	All
Application	Plataformatec	Devise	2.1.2	All	All	All
Application	Plataformatec	Devise	2.2.0	All	All	All
Application	Plataformatec	Devise	2.2.1	All	All	All
Application	Plataformatec	Devise	2.2.2	All	All	All
Application	Ruby-lang	Ruby	All	All	All	All
Application	Ruby-lang	Ruby	All	All	All	All

References						
Reference				Source	Link	
Security announcement: Devise v2.2.3, v2.1.3, v2.0.5 and v1.5.4 released Plataformatec Blog				CONFIRM	blog.plataformatec.com	
Update Gemfile for recent Devise security vulnerability (CVE-2013-0233) · Issue #261 · Snorby/snorby · GitHub				MISC	github.com	
Devise CVE-2013-0233 Security Bypass Vulnerability				BID	www.securityfocus.com/bid/60307	
oss-security - Re: CVE request for 'devise' ruby gem				MLIST	www.openwall.com/lists/oss-security	
MySQL madness and Rails Lands of Packets				MISC	www.phenoelit.org/rails.html	
Ruby on Rails Devise Authentication Password Reset Metasploit Exploit Database (DB)				MISC	www.metasploit.com/docs/0-9/44661/devise_authentication_password_reset.rb	
openSUSE-SU-2013:0374-1: moderate: rubygem-devise: updated to version 1.				SUSE	lists.opensuse.org/archives/list/opensuse-security@opensuse.org/message/5333333333333333	
CVE Program record				CVE.ORG	www.cve.org/CVE/nvd/cve-2013-0233	
NVD vulnerability detail				NVD	nvd.nist.gov/vuln/detail/CVE-2013-0233	

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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