



CVE-2013-1756

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

Summary

CVE	CVE-2013-1756
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-09 19:55:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The Dragonfly gem 0.7 before 0.8.6 and 0.9.x before 0.9.13 for Ruby, when used with Ruby on Rails, allows remote attackers

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: CWE-94 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mark Evans	Dragonfly Gem	0.7.0	All	All	All

Application	Mark Evans	Dragonfly Gem	0.7.1	All	All	All
Application	Mark Evans	Dragonfly Gem	0.7.2	All	All	All
Application	Mark Evans	Dragonfly Gem	0.7.3	All	All	All
Application	Mark Evans	Dragonfly Gem	0.7.4	All	All	All
Application	Mark Evans	Dragonfly Gem	0.7.5	All	All	All
Application	Mark Evans	Dragonfly Gem	0.7.6	All	All	All
Application	Mark Evans	Dragonfly Gem	0.7.7	All	All	All
Application	Mark Evans	Dragonfly Gem	0.8.0	All	All	All
Application	Mark Evans	Dragonfly Gem	0.8.1	All	All	All
Application	Mark Evans	Dragonfly Gem	0.8.2	All	All	All
Application	Mark Evans	Dragonfly Gem	0.8.4	All	All	All
Application	Mark Evans	Dragonfly Gem	0.8.5	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.0	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.1	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.10	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.11	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.12	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.2	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.3	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.4	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.5	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.6	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.7	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.8	All	All	All
Application	Mark Evans	Dragonfly Gem	0.9.9	All	All	All
Application	Ruby On Rails	Ruby On Rails	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference					Source	
IBM X-Force Exchange					af854a3a-2127-422b-91a1-100000000000	
Ruby dragonfly Gem CVE-2013-1756 Remote Arbitrary Code Execution Vulnerability					af854a3a-2127-422b-91a1-100000000000	
security update note · markevans/dragonfly@ a8775aa · GitHub					af854a3a-2127-422b-91a1-100000000000	
Google Groups					af854a3a-2127-422b-91a1-100000000000	

Google Groups	af854a3a-2127-422b-91a1-8b54a3a-2127-422b-91a1
Security Advisory SA52380 - Ruby dragonfly Gem Ruby on Rails Arbitrary Code Execution Vulnerability - Secunia	af854a3a-2127-422b-91a1-8b54a3a-2127-422b-91a1
Google Groups	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)