



CVE-2013-1908

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

Summary

CVE	CVE-2013-1908
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-07-16 18:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The Commons Wikis module before 7.x-3.1 for Drupal, as used in the Commons module before 7.x-3.1, does not properly r

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Acquia	Commons	7.x-3.x	dev	All	All

Application	Acquia	Commons	All	All	All	All
Application	Commons Wikis Project	Commons Wikis	7.x-3.x	dev	All	All
Application	Commons Wikis Project	Commons Wikis	All	All	All	All
Application	Drupal	Drupal	-	All	All	All

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

References	
Reference	Source
Drupal Common Wikis 7.x Access Bypass / Privilege Escalation ~ Packet Storm	af854a3a-2127-422b-91a
About Secunia Research Flexera	af854a3a-2127-422b-91a
Full Disclosure: [Security-news] SA-CONTRIB-2013-039 - Commons Wikis - Access bypass & Privilege escalation	af854a3a-2127-422b-91a
commons_wikis 7.x-3.1 drupal.org	af854a3a-2127-422b-91a
SA-CONTRIB-2013-039 - Commons Wikis - Access bypass & Privilege escalation drupal.org	af854a3a-2127-422b-91a
osvdb.org/91747	af854a3a-2127-422b-91a
Security Advisory SA52795 - Drupal Commons Module Two Security Bypass Security Issues - Secunia	af854a3a-2127-422b-91a
commons 7.x-3.1 drupal.org	af854a3a-2127-422b-91a
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.