



CVE-2012-2706

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

Summary

CVE	CVE-2012-2706
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-27 00:55:00 UTC
Updated	2017-08-29 01:31:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the Post Affiliate Pro (PAP) module for Drupal allows remote attackers to inject ar

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Drupal	Drupal	-	All	All	All
Application	Drupal	Drupal	-	All	All	All
Application	Peter Pokrivcak	Post Affiliate Pro	-	All	All	All
Application	Peter Pokrivcak	Post Affiliate Pro	-	All	All	All

References

Reference	Source	Link
SA-CONTRIB-2012-079 - Post Affiliate Pro - Cross Site Scripting (XSS) and Access Bypass - Unsupported drupal.org	MISC	drupal.
IBM X-Force Exchange	XF	exchar
Drupal Post Affiliate Pro Cross Site Scripting and Access Security Bypass Vulnerabilities	BID	www.s
oss-security - Re: CVE Request for Drupal contributed modules	MLIST	www.o
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

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](#)