CVE-2009-2079

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-2079
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-06-16 19:30:00 UTC
Updated	2009-06-17 04:00:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the administrative page interface in Taxonomy manager 5.x before 5.x-1.2 and 6.x

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	All
Application	Drupal	Drupal	All	All	All	All
Application	Drupal	Taxonomy Manager	5.x-1.0	All	All	All
Application	Drupal	Taxonomy Manager	5.x-1.1	All	All	All
Application	Drupal	Taxonomy Manager	6.x-1.0	All	All	All
Application	Drupal	Taxonomy Manager	6.x-1.0-beta1	All	All	All
Application	Drupal	Taxonomy Manager	6.x-1.0-beta2	All	All	All
Application	Drupal	Taxonomy Manager	5.x-1.0	All	All	All
Application	Drupal	Taxonomy Manager	5.x-1.1	All	All	All
Application	Drupal	Taxonomy Manager	6.x-1.0	All	All	All
Application	Drupal	Taxonomy Manager	6.x-1.0-beta1	All	All	All
Application	Drupal	Taxonomy Manager	6.x-1.0-beta2	All	All	All

References

Reference	Source	Link	Tags
taxonomy_manager 6.x-1.1 | drupal.org	CONFIRM	drupal.org	Patch
Drupal Taxonomy Manager Module Script Insertion Vulnerability - Secunia.com	SECUNIA	secunia.com	Vendor Advisc

Drupal Taxonomy Manager Administrative Page HTML Injection Vulnerability	BID	www.securityfocus.com	
Drupal 6 Taxonomy Manager XSS Vulnerability | Linux/Apache/MySQL/PHP Security	MISC	lampsecurity.org	Exploit
taxonomy_manager 5.x-1.2 | drupal.org	CONFIRM	drupal.org	Patch
SA-CONTRIB-2009-034 - Taxonomy manager - Cross site scripting | drupal.org	CONFIRM	drupal.org	Patch, Vendor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**