



CVE-2015-4389

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

Summary

CVE	CVE-2015-4389
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-15 14:59:00 UTC
Updated	2016-06-09 21:29:00 UTC
Description	The Open Graph Importer (og_tag_importer) 7.x-1.x for Drupal does not properly check the create permission for content ty

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Open Graph Importer Project	Open Graph Importer	7.x-1.0	All	All	All
Application	Open Graph Importer Project	Open Graph Importer	7.x-1.0	All	All	All

References

Reference	Source	Link
oss-security - CVE requests for Drupal contributed modules (from SA-CONTRIB-2015-034 to SA-CONTRIB-2015-099)	MLIST	www.oss-security.org
Drupal Open Graph Importer Module Access Bypass Vulnerability	BID	www.securityfocus.com
Open Graph Importer - Moderately Critical - Access bypass - Unsupported - SA-CONTRIB-2015-092 Drupal.org	MISC	www.drupal.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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