



# CVE-2012-2711

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

## Summary

<b>CVE</b>	CVE-2012-2711
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-06-27 00:55:00 UTC
<b>Updated</b>	2017-08-29 01:31:00 UTC
<b>Description</b>	Multiple cross-site scripting (XSS) vulnerabilities in the Taxonomy List module 6.x-1.x before 6.x-1.4 for Drupal allow remote

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Drupal</a>	<a href="#">Drupal</a>	-	All	All	All
Application	<a href="#">Drupal</a>	<a href="#">Drupal</a>	-	All	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.0	All	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.0-beta1	All	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.1	All	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.2	All	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.2	dev	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.3	All	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.x-dev	All	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.0	All	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.0-beta1	All	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.1	All	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.2	All	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.2	dev	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.3	All	All	All
Application	<a href="#">Nancy Wichmann</a>	<a href="#">Taxonomy List</a>	6.x-1.x-dev	All	All	All

## References

Reference	Source	Link	Tags
SA-CONTRIB-2012-083 - Taxonomy List - Cross Site Scripting (XSS)   drupal.org	MISC	<a href="https://drupal.org">drupal.org</a>	Patch, Ver
About Secunia Research   Flexera	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Vendor Ad
Drupal Taxonomy List Module Cross Site Scripting Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Patch
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
taxonomy_list 6.x-1.4   drupal.org	CONFIRM	<a href="https://drupal.org">drupal.org</a>	Patch
82164	OSVDB	<a href="https://www.osvdb.org">www.osvdb.org</a>	
oss-security - Re: CVE Request for Drupal contributed modules	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	
Log in   Drupal.org	CONFIRM	<a href="https://drupalcode.org">drupalcode.org</a>	Exploit, Pa
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical,

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**