



CVE-2013-4380

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

Summary

CVE	CVE-2013-4380
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-20 14:55:00 UTC
Updated	2014-05-21 18:44:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the MediaFront module 6.x-1.x before 6.x-1.6, 7.x-1.x before 7.x-1.6, and 7.x-2.x before 7.x-2.6

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	Mediafront	Mediafront	6.x-1.0	All	All	All
Application	Mediafront	Mediafront	6.x-1.0	beta1	All	All
Application	Mediafront	Mediafront	6.x-1.0	beta2	All	All
Application	Mediafront	Mediafront	6.x-1.0	beta4	All	All
Application	Mediafront	Mediafront	6.x-1.0	beta5	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc1	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc2	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc3	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc4	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc5	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc6	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc7	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc8	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc9	All	All
Application	Mediafront	Mediafront	6.x-1.1	All	All	All

Application	Mediafront	Mediafront	6.x-1.2	All	All	All
Application	Mediafront	Mediafront	6.x-1.3	All	All	All
Application	Mediafront	Mediafront	6.x-1.5	All	All	All
Application	Mediafront	Mediafront	6.x-1.x	dev	All	All
Application	Mediafront	Mediafront	7.x-1.0	-	All	All
Application	Mediafront	Mediafront	7.x-1.0	beta1	All	All
Application	Mediafront	Mediafront	7.x-1.0	beta2	All	All
Application	Mediafront	Mediafront	7.x-1.0	beta3	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc1	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc2	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc3	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc4	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc5	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc6	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc7	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc8	All	All
Application	Mediafront	Mediafront	7.x-1.1	All	All	All
Application	Mediafront	Mediafront	7.x-1.2	All	All	All
Application	Mediafront	Mediafront	7.x-1.3	All	All	All
Application	Mediafront	Mediafront	7.x-1.4	All	All	All
Application	Mediafront	Mediafront	7.x-1.5	All	All	All
Application	Mediafront	Mediafront	7.x-1.x	dev	All	All
Application	Mediafront	Mediafront	7.x-2.0	-	All	All
Application	Mediafront	Mediafront	7.x-2.0	alpha1	All	All
Application	Mediafront	Mediafront	7.x-2.0	alpha2	All	All
Application	Mediafront	Mediafront	7.x-2.0	alpha3	All	All
Application	Mediafront	Mediafront	7.x-2.0	alpha4	All	All
Application	Mediafront	Mediafront	7.x-2.0	alpha5	All	All
Application	Mediafront	Mediafront	7.x-2.0	beta1	All	All
Application	Mediafront	Mediafront	7.x-2.0	beta2	All	All
Application	Mediafront	Mediafront	7.x-2.0	beta4	All	All
Application	Mediafront	Mediafront	7.x-2.0	beta5	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc1	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc2	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc3	All	All

Application	Mediafront	Mediafront	7.x-2.0	rc4	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc5	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc6	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc7	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc8	All	All
Application	Mediafront	Mediafront	7.x-2.x	dev	All	All
Application	Mediafront	Mediafront	6.x-1.0	All	All	All
Application	Mediafront	Mediafront	6.x-1.0	beta1	All	All
Application	Mediafront	Mediafront	6.x-1.0	beta2	All	All
Application	Mediafront	Mediafront	6.x-1.0	beta4	All	All
Application	Mediafront	Mediafront	6.x-1.0	beta5	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc1	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc2	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc3	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc4	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc5	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc6	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc7	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc8	All	All
Application	Mediafront	Mediafront	6.x-1.0	rc9	All	All
Application	Mediafront	Mediafront	6.x-1.1	All	All	All
Application	Mediafront	Mediafront	6.x-1.2	All	All	All
Application	Mediafront	Mediafront	6.x-1.3	All	All	All
Application	Mediafront	Mediafront	6.x-1.5	All	All	All
Application	Mediafront	Mediafront	6.x-1.x	dev	All	All
Application	Mediafront	Mediafront	7.x-1.0	-	All	All
Application	Mediafront	Mediafront	7.x-1.0	beta1	All	All
Application	Mediafront	Mediafront	7.x-1.0	beta2	All	All
Application	Mediafront	Mediafront	7.x-1.0	beta3	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc1	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc2	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc3	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc4	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc5	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc6	All	All

Application	Mediafront	Mediafront	7.x-1.0	rc7	All	All
Application	Mediafront	Mediafront	7.x-1.0	rc8	All	All
Application	Mediafront	Mediafront	7.x-1.1	All	All	All
Application	Mediafront	Mediafront	7.x-1.2	All	All	All
Application	Mediafront	Mediafront	7.x-1.3	All	All	All
Application	Mediafront	Mediafront	7.x-1.4	All	All	All
Application	Mediafront	Mediafront	7.x-1.5	All	All	All
Application	Mediafront	Mediafront	7.x-1.x	dev	All	All
Application	Mediafront	Mediafront	7.x-2.0	-	All	All
Application	Mediafront	Mediafront	7.x-2.0	alpha1	All	All
Application	Mediafront	Mediafront	7.x-2.0	alpha2	All	All
Application	Mediafront	Mediafront	7.x-2.0	alpha3	All	All
Application	Mediafront	Mediafront	7.x-2.0	alpha4	All	All
Application	Mediafront	Mediafront	7.x-2.0	alpha5	All	All
Application	Mediafront	Mediafront	7.x-2.0	beta1	All	All
Application	Mediafront	Mediafront	7.x-2.0	beta2	All	All
Application	Mediafront	Mediafront	7.x-2.0	beta4	All	All
Application	Mediafront	Mediafront	7.x-2.0	beta5	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc1	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc2	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc3	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc4	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc5	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc6	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc7	All	All
Application	Mediafront	Mediafront	7.x-2.0	rc8	All	All
Application	Mediafront	Mediafront	7.x-2.x	dev	All	All

References						
Reference			Source	Link	Tags	
SA-CONTRIB-2013-074 - MediaFront - Cross Site Scripting (XSS) Drupal.org			MISC	drupal.org	Patch, Vendor Advisory	
mediafront 7.x-2.1 Drupal.org			CONFIRM	drupal.org	Patch	
oss-security - Re: CVE request for Drupal contributed modules			MLIST	www.openwall.com		
mediafront 7.x-1.6 Drupal.org			CONFIRM	drupal.org	Patch	
mediafront 6.x-1.6 Drupal.org			CONFIRM	drupal.org	Patch	
CVE Program record			CVE.ORG	www.cve.org	canonical	

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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://cve.mitre.org). 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