



Published on: 11/17/2015 12:00:00 AM UTC

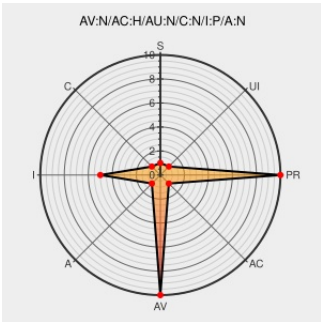
Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8233

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Mayo](#) from [Mayo Project](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the MAYO theme 7.x-1.x before 7.x-1.4 and 7.x-2.x before 7.x-2.6 for Drupal allows remote administrators with the "Administer themes" permission to inject arbitrary web script or HTML via unspecified vectors related to theme settings.

CVE-2015-8233 has been assigned by  cve@mitre.org to track the vulnerability

CVSS2 Score: 2.6 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
MAYO theme - Moderately Critical - Cross Site Scripting (XSS) - SA-CONTRIB-2015-164 Drupal.org	Patch Vendor Advisory www.drupal.org text/html	 MISC www.drupal.org/node/2613424
mayo 7.x-2.6 Drupal.org	Patch www.drupal.org text/html	 CONFIRM www.drupal.org/node/2613048
mayo 7.x-1.4 Drupal.org	Patch www.drupal.org text/html	 CONFIRM www.drupal.org/node/2613046

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mayo Project	Mayo	7.x-1.0	All	All	All
Application	Mayo Project	Mayo	7.x-1.1	All	All	All
Application	Mayo Project	Mayo	7.x-1.2	All	All	All
Application	Mayo Project	Mayo	7.x-1.3	All	All	All
Application	Mayo Project	Mayo	7.x-2.0	All	All	All
Application	Mayo Project	Mayo	7.x-2.0	alpha1	All	All
Application	Mayo Project	Mayo	7.x-2.0	alpha2	All	All
Application	Mayo Project	Mayo	7.x-2.0	alpha3	All	All
Application	Mayo Project	Mayo	7.x-2.0	beta1	All	All
Application	Mayo Project	Mayo	7.x-2.0	beta2	All	All
Application	Mayo Project	Mayo	7.x-2.0	rc1	All	All
Application	Mayo Project	Mayo	7.x-2.0	rc2	All	All
Application	Mayo Project	Mayo	7.x-2.1	All	All	All
Application	Mayo Project	Mayo	7.x-2.2	All	All	All
Application	Mayo Project	Mayo	7.x-2.3	All	All	All
Application	Mayo Project	Mayo	7.x-2.4	All	All	All
Application	Mayo Project	Mayo	7.x-2.5	All	All	All
Application	Mayo Project	Mayo	7.x-1.0	All	All	All
Application	Mayo Project	Mayo	7.x-1.1	All	All	All
Application	Mayo Project	Mayo	7.x-1.2	All	All	All
Application	Mayo Project	Mayo	7.x-1.3	All	All	All
Application	Mayo Project	Mayo	7.x-2.0	All	All	All
Application	Mayo Project	Mayo	7.x-2.0	alpha1	All	All
Application	Mayo Project	Mayo	7.x-2.0	alpha2	All	All
Application	Mayo Project	Mayo	7.x-2.0	alpha3	All	All
Application	Mayo Project	Mayo	7.x-2.0	beta1	All	All
Application	Mayo Project	Mayo	7.x-2.0	beta2	All	All
Application	Mayo Project	Mayo	7.x-2.0	rc1	All	All
Application	Mayo Project	Mayo	7.x-2.0	rc2	All	All

Application	Mayo Project	Mayo	7.x-2.1	All	All	All
Application	Mayo Project	Mayo	7.x-2.2	All	All	All
Application	Mayo Project	Mayo	7.x-2.3	All	All	All
Application	Mayo Project	Mayo	7.x-2.4	All	All	All
Application	Mayo Project	Mayo	7.x-2.5	All	All	All
cpe:2.3:a:mayo_project:mayo:7.x-1.0:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-1.1:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-1.2:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-1.3:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.0:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.0:alpha1:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.0:alpha2:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.0:alpha3:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.0:beta1:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.0:beta2:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.0:rc1:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.0:rc2:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.1:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.2:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.3:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.4:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.5:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-1.0:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-1.1:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-1.2:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-1.3:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.0:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.0:alpha1:***:drupal:**:						
cpe:2.3:a:mayo_project:mayo:7.x-2.0:alpha2:***:drupal:**:						

cpe:2.3:a:maya_project:maya:7.x-2.0:alpha3:*:*:*:drupal:*:*:
cpe:2.3:a:maya_project:maya:7.x-2.0:beta1:*:*:*:drupal:*:*:
cpe:2.3:a:maya_project:maya:7.x-2.0:beta2:*:*:*:drupal:*:*:
cpe:2.3:a:maya_project:maya:7.x-2.0:rc1:*:*:*:drupal:*:*:
cpe:2.3:a:maya_project:maya:7.x-2.0:rc2:*:*:*:drupal:*:*:
cpe:2.3:a:maya_project:maya:7.x-2.1:*:*:*:drupal:*:*:
cpe:2.3:a:maya_project:maya:7.x-2.2:*:*:*:drupal:*:*:
cpe:2.3:a:maya_project:maya:7.x-2.3:*:*:*:drupal:*:*:
cpe:2.3:a:maya_project:maya:7.x-2.4:*:*:*:drupal:*:*:
cpe:2.3:a:maya_project:maya:7.x-2.5:*:*:*:drupal:*:*:

No vendor comments have been submitted for this CVE