

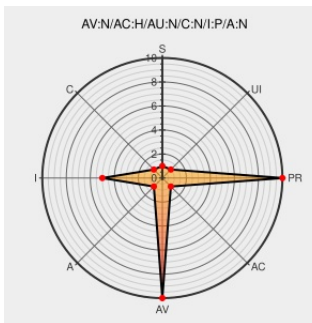


CVE-2012-5588

Published on: 12/26/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:20 PM UTC

CVE-2012-5588

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The Email Field module 6.x-1.x before 6.x-1.3 for Drupal, when using a field permission module and the field contact field formatter is set to the full or teaser display mode, does not properly check permissions, which allows remote attackers to email the stored address via unspecified vectors.

CVE-2012-5588 has been assigned by secalert@redhat.com 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
email 6.x-1.4 drupal.org	Patch drupal.org text/html	CONFIRM drupal.org/node/1852612
SA-CONTRIB-2012-169 - Email Field - Cross Site Scripting and Access bypass drupal.org	Patch Vendor Advisory drupal.org text/html	MISC drupal.org/node/1853214
oss-security - Re: CVE request for Drupal contributed modules	www.openwall.com text/html	MLIST [oss-security] 20121128 Re: CVE request for Drupal contributed modules

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,

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Drupal	Drupal	-	All	All	All
Application	Drupal	Drupal	-	All	All	All
Application	Epiqo	Email	6.x-1.0	All	All	All
Application	Epiqo	Email	6.x-1.0	rc1	All	All
Application	Epiqo	Email	6.x-1.1	All	All	All
Application	Epiqo	Email	6.x-1.2	All	All	All
Application	Epiqo	Email	6.x-1.x	dev	All	All
Application	Epiqo	Email	6.x-1.0	All	All	All
Application	Epiqo	Email	6.x-1.0	rc1	All	All
Application	Epiqo	Email	6.x-1.1	All	All	All
Application	Epiqo	Email	6.x-1.2	All	All	All
Application	Epiqo	Email	6.x-1.x	dev	All	All

cpe:2.3:a:drupal:drupal:-:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:-:*:*:*:*:*:

cpe:2.3:a:epiqo:email:6.x-1.0:*:*:*:*:*:

cpe:2.3:a:epiqo:email:6.x-1.0:rc1:*:*:*:*:*:

cpe:2.3:a:epiqo:email:6.x-1.1:*:*:*:*:*:

cpe:2.3:a:epiqo:email:6.x-1.2:*:*:*:*:*:

cpe:2.3:a:epiqo:email:6.x-1.x:dev:*:*:*:*:*:

cpe:2.3:a:epiqo:email:6.x-1.0:*:*:*:*:*:

cpe:2.3:a:epiqo:email:6.x-1.0:rc1:*:*:*:*:*:

cpe:2.3:a:epiqo:email:6.x-1.1:*:*:*:*:*:

cpe:2.3:a:epiqo:email:6.x-1.2:*:*:*:*:*:

cpe:2.3:a:epiqo:email:6.x-1.x:dev:*:*:*:*:*:

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)