

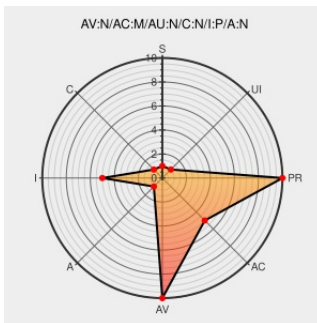


CVE-2009-1047

Published on: 03/23/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:26 PM UTC

CVE-2009-1047

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

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

Cross-site scripting (XSS) vulnerability in the Send by e-mail module in the "Printer, e-mail and PDF versions" module 5.x before 5.x-4.4 and 6.x before 6.x-1.4, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via vectors involving outbound HTML e-mail.

CVE-2009-1047 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
SA-CONTRIB-2009-012 - Printer, e-mail and PDF versions - Unrestricted e-mailing (spam) drupal.org	Patch Vendor Advisory drupal.org text/html	CONFIRM drupal.org/node/406516
No Description Provided	osvdb.org	OSVDB 52852
	Inactive Link Not Archived	

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	Drupal	Drupal	All	All	All	All
Application	Drupal	Drupal	All	All	All	All
Application	Drupal	Print	5.x	All	All	All
Application	Drupal	Print	5.x-1.0	All	All	All
Application	Drupal	Print	5.x-1.1	All	All	All
Application	Drupal	Print	5.x-1.2	All	All	All
Application	Drupal	Print	5.x-1.x-dev	All	All	All
Application	Drupal	Print	5.x-2.1	All	All	All
Application	Drupal	Print	5.x-2.2	All	All	All
Application	Drupal	Print	5.x-2.x-dev	All	All	All
Application	Drupal	Print	5.x-3.0	All	All	All
Application	Drupal	Print	5.x-3.1	All	All	All
Application	Drupal	Print	5.x-3.2	All	All	All
Application	Drupal	Print	5.x-3.3	All	All	All
Application	Drupal	Print	5.x-3.4	All	All	All
Application	Drupal	Print	5.x-3.5	All	All	All
Application	Drupal	Print	5.x-3.6	All	All	All
Application	Drupal	Print	5.x-3.7	All	All	All
Application	Drupal	Print	5.x-4.0	All	All	All
Application	Drupal	Print	5.x-4.1	All	All	All
Application	Drupal	Print	5.x-4.2	All	All	All
Application	Drupal	Print	5.x-4.3	All	All	All
Application	Drupal	Print	5.x-4.x	dev	All	All
Application	Drupal	Print	6.x-1.0	All	All	All
Application	Drupal	Print	6.x-1.0-rc3	All	All	All
Application	Drupal	Print	6.x-1.0-rc4	All	All	All
Application	Drupal	Print	6.x-1.0-rc5	All	All	All
Application	Drupal	Print	6.x-1.0-rc8	All	All	All
Application	Drupal	Print	6.x-1.0-rc9	All	All	All
Application	Drupal	Print	6.x-1.1	All	All	All
Application	Drupal	Print	6.x-1.2	All	All	All

Application	Drupal	Print	6.x-1.3	All	All	All
Application	Drupal	Print	6.x-1.4	All	All	All
Application	Drupal	Print	6.x-1.x-dev	All	All	All
Application	Drupal	Print	5.x	All	All	All
Application	Drupal	Print	5.x-1.0	All	All	All
Application	Drupal	Print	5.x-1.1	All	All	All
Application	Drupal	Print	5.x-1.2	All	All	All
Application	Drupal	Print	5.x-1.x-dev	All	All	All
Application	Drupal	Print	5.x-2.1	All	All	All
Application	Drupal	Print	5.x-2.2	All	All	All
Application	Drupal	Print	5.x-2.x-dev	All	All	All
Application	Drupal	Print	5.x-3.0	All	All	All
Application	Drupal	Print	5.x-3.1	All	All	All
Application	Drupal	Print	5.x-3.2	All	All	All
Application	Drupal	Print	5.x-3.3	All	All	All
Application	Drupal	Print	5.x-3.4	All	All	All
Application	Drupal	Print	5.x-3.5	All	All	All
Application	Drupal	Print	5.x-3.6	All	All	All
Application	Drupal	Print	5.x-3.7	All	All	All
Application	Drupal	Print	5.x-4.0	All	All	All
Application	Drupal	Print	5.x-4.1	All	All	All
Application	Drupal	Print	5.x-4.2	All	All	All
Application	Drupal	Print	5.x-4.3	All	All	All
Application	Drupal	Print	5.x-4.x	dev	All	All
Application	Drupal	Print	6.x-1.0	All	All	All
Application	Drupal	Print	6.x-1.0-rc3	All	All	All
Application	Drupal	Print	6.x-1.0-rc4	All	All	All
Application	Drupal	Print	6.x-1.0-rc5	All	All	All
Application	Drupal	Print	6.x-1.0-rc8	All	All	All
Application	Drupal	Print	6.x-1.0-rc9	All	All	All
Application	Drupal	Print	6.x-1.1	All	All	All
Application	Drupal	Print	6.x-1.2	All	All	All
Application	Drupal	Print	6.x-1.3	All	All	All
Application	Drupal	Print	6.x-1.4	All	All	All
Application	Drupal	Print	6.x-1.x-dev	All	All	All

cpe:2.3:a:drupal:drupal:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-1.0:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-1.1:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-1.2:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-1.x-dev:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-2.1:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-2.2:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-2.x-dev:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-3.0:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-3.1:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-3.2:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-3.3:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-3.4:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-3.5:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-3.6:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-3.7:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-4.0:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-4.1:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-4.2:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-4.3:*:*:*:*:*:
cpe:2.3:a:drupal:print:5.x-4.x-dev:*:*:*:*:*:
cpe:2.3:a:drupal:print:6.x-1.0:*:*:*:*:*:
cpe:2.3:a:drupal:print:6.x-1.0-rc3:*:*:*:*:*:
cpe:2.3:a:drupal:print:6.x-1.0-rc4:*:*:*:*:*:
cpe:2.3:a:drupal:print:6.x-1.0-rc5:*:*:*:*:*:
cpe:2.3:a:drupal:print:6.x-1.0-rc8:*:*:*:*:*:
cpe:2.3:a:drupal:print:6.x-1.0-rc9:*:*:*:*:*:

cpe:2.3:a:drupal:print:6.x-1.1:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:6.x-1.2:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:6.x-1.3:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:6.x-1.4:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:6.x-1.x-dev:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-1.0:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-1.1:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-1.2:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-1.x-dev:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-2.1:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-2.2:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-2.x-dev:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-3.0:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-3.1:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-3.2:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-3.3:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-3.4:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-3.5:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-3.6:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-3.7:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-4.0:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-4.1:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-4.2:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-4.3:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:5.x-4.x-dev:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:6.x-1.0:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:a:drupal:print:6.x-1.0-rc3:~::~~::~~::~~::~~::~~::~~::

cpe:2.3:a:drupal:print:6.x-1.0-rc4:*****:
cpe:2.3:a:drupal:print:6.x-1.0-rc5:*****:
cpe:2.3:a:drupal:print:6.x-1.0-rc8:*****:
cpe:2.3:a:drupal:print:6.x-1.0-rc9:*****:
cpe:2.3:a:drupal:print:6.x-1.1:*****:
cpe:2.3:a:drupal:print:6.x-1.2:*****:
cpe:2.3:a:drupal:print:6.x-1.3:*****:
cpe:2.3:a:drupal:print:6.x-1.4:*****:
cpe:2.3:a:drupal:print:6.x-1.x-dev:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)