



CVE-2012-5540

Published on: 12/03/2012 12:00:00 AM UTC

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

CVE-2012-5540

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Multiple cross-site scripting (XSS) vulnerabilities in the Hostip module 6.x-2.x before 6.x-2.2 and 7.x-2.x before 7.x-2.2 for Drupal allow remote attackers with control of hostip.info to inject arbitrary web script or HTML via unspecified vectors.

CVE-2012-5540 has been assigned by secalert@redhat.com 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

hostip 7.x-1.2 | drupal.org

[Patch](#)
[drupal.org](#)
[text/html](#)

[CONFIRM drupal.org/node/1802048](#)

hostip 6.x-1.2 | drupal.org

[Patch](#)
[drupal.org](#)
[text/html](#)

[CONFIRM drupal.org/node/1802046](#)

SA-CONTRIB-2012-149 - Hostip - Cross Site Scripting (XSS) | drupal.org

[Patch](#)
[Vendor Advisory](#)
[drupal.org](#)
[text/html](#)

[MISC drupal.org/node/1802218](#)

oss-security - Re: CVE Request for Drupal Contributed Modules

[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20121120 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

By selecting these links, you may be leaving CVEreport website. 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
Application	Drupal	Drupal	-	All	All	All
Application	Tekritissoftware	Hostip	6.x-2.0	All	All	All
Application	Tekritissoftware	Hostip	6.x-2.1	All	All	All
Application	Tekritissoftware	Hostip	7.x-2.0	All	All	All
Application	Tekritissoftware	Hostip	7.x-2.1	All	All	All
Application	Tekritissoftware	Hostip	6.x-2.0	All	All	All
Application	Tekritissoftware	Hostip	6.x-2.1	All	All	All
Application	Tekritissoftware	Hostip	7.x-2.0	All	All	All
Application	Tekritissoftware	Hostip	7.x-2.1	All	All	All
cpe:2.3:a:drupal:drupal:-:*:*:*:*:*:						
cpe:2.3:a:drupal:drupal:-:*:*:*:*:*:						
cpe:2.3:a:tekritissoftware:hostip:6.x-2.0:*:*:*:*:*:						
cpe:2.3:a:tekritissoftware:hostip:6.x-2.1:*:*:*:*:*:						
cpe:2.3:a:tekritissoftware:hostip:7.x-2.0:*:*:*:*:*:						
cpe:2.3:a:tekritissoftware:hostip:7.x-2.1:*:*:*:*:*:						
cpe:2.3:a:tekritissoftware:hostip:6.x-2.0:*:*:*:*:*:						
cpe:2.3:a:tekritissoftware:hostip:6.x-2.1:*:*:*:*:*:						
cpe:2.3:a:tekritissoftware:hostip:7.x-2.0:*:*:*:*:*:						
cpe:2.3:a:tekritissoftware:hostip:7.x-2.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)