



CVE-2013-6389

Published on: 12/07/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:37 PM UTC

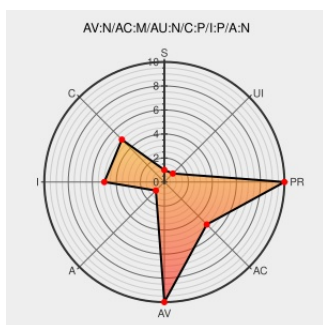
CVE-2013-6389

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Open redirect vulnerability in the Overlay module in Drupal 7.x before 7.24 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.

CVE-2013-6389 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5.8 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

NONE

CVE References

Description

Tags

Link

oss-security - SA-CORE-2013-003 - Drupal core - Multiple vulnerabilities

[www.openwall.com
text/html](http://www.openwall.com/text/html)

[MLIST \[oss-security\] 20131122 SA-CORE-2013-003 - Drupal core - Multiple vulnerabilities](#)

Debian -- Security Information -- DSA-2804-1 drupal7

[www.debian.org
Deprecated Link
text/html](http://www.debian.org/Deprecated Link)

[DEBIAN DSA-2804](#)

SA-CORE-2013-003 - Drupal core - Multiple vulnerabilities | Drupal.org

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

[CONFIRM drupal.org/SA-CORE-2013-003](http://drupal.org/SA-CORE-2013-003)

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

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	7.0	All	All	All
Application	Drupal	Drupal	7.0	alpha1	All	All
Application	Drupal	Drupal	7.0	alpha2	All	All
Application	Drupal	Drupal	7.0	alpha3	All	All
Application	Drupal	Drupal	7.0	alpha4	All	All
Application	Drupal	Drupal	7.0	alpha5	All	All
Application	Drupal	Drupal	7.0	alpha6	All	All
Application	Drupal	Drupal	7.0	alpha7	All	All
Application	Drupal	Drupal	7.0	beta1	All	All
Application	Drupal	Drupal	7.0	beta2	All	All
Application	Drupal	Drupal	7.0	beta3	All	All
Application	Drupal	Drupal	7.0	dev	All	All
Application	Drupal	Drupal	7.0	rc1	All	All
Application	Drupal	Drupal	7.0	rc2	All	All
Application	Drupal	Drupal	7.0	rc3	All	All
Application	Drupal	Drupal	7.0	rc4	All	All
Application	Drupal	Drupal	7.1	All	All	All
Application	Drupal	Drupal	7.10	All	All	All
Application	Drupal	Drupal	7.11	All	All	All
Application	Drupal	Drupal	7.12	All	All	All
Application	Drupal	Drupal	7.13	All	All	All
Application	Drupal	Drupal	7.14	All	All	All
Application	Drupal	Drupal	7.15	All	All	All
Application	Drupal	Drupal	7.16	All	All	All
Application	Drupal	Drupal	7.17	All	All	All
Application	Drupal	Drupal	7.18	All	All	All
Application	Drupal	Drupal	7.19	All	All	All
Application	Drupal	Drupal	7.2	All	All	All
Application	Drupal	Drupal	7.20	All	All	All
Application	Drupal	Drupal	7.21	All	All	All

Application	Drupal	Drupal	7.22	All	All	All
Application	Drupal	Drupal	7.23	All	All	All
Application	Drupal	Drupal	7.3	All	All	All
Application	Drupal	Drupal	7.4	All	All	All
Application	Drupal	Drupal	7.5	All	All	All
Application	Drupal	Drupal	7.6	All	All	All
Application	Drupal	Drupal	7.7	All	All	All
Application	Drupal	Drupal	7.8	All	All	All
Application	Drupal	Drupal	7.9	All	All	All
Application	Drupal	Drupal	7.x-dev	All	All	All
Application	Drupal	Drupal	7.0	All	All	All
Application	Drupal	Drupal	7.0	alpha1	All	All
Application	Drupal	Drupal	7.0	alpha2	All	All
Application	Drupal	Drupal	7.0	alpha3	All	All
Application	Drupal	Drupal	7.0	alpha4	All	All
Application	Drupal	Drupal	7.0	alpha5	All	All
Application	Drupal	Drupal	7.0	alpha6	All	All
Application	Drupal	Drupal	7.0	alpha7	All	All
Application	Drupal	Drupal	7.0	beta1	All	All
Application	Drupal	Drupal	7.0	beta2	All	All
Application	Drupal	Drupal	7.0	beta3	All	All
Application	Drupal	Drupal	7.0	dev	All	All
Application	Drupal	Drupal	7.0	rc1	All	All
Application	Drupal	Drupal	7.0	rc2	All	All
Application	Drupal	Drupal	7.0	rc3	All	All
Application	Drupal	Drupal	7.0	rc4	All	All
Application	Drupal	Drupal	7.1	All	All	All
Application	Drupal	Drupal	7.10	All	All	All
Application	Drupal	Drupal	7.11	All	All	All
Application	Drupal	Drupal	7.12	All	All	All
Application	Drupal	Drupal	7.13	All	All	All
Application	Drupal	Drupal	7.14	All	All	All
Application	Drupal	Drupal	7.15	All	All	All
Application	Drupal	Drupal	7.16	All	All	All
Application	Drupal	Drupal	7.17	All	All	All
Application	Drupal	Drupal	7.18	All	All	All

Application	Drupal	Drupal	7.19	All	All	All
Application	Drupal	Drupal	7.2	All	All	All
Application	Drupal	Drupal	7.20	All	All	All
Application	Drupal	Drupal	7.21	All	All	All
Application	Drupal	Drupal	7.22	All	All	All
Application	Drupal	Drupal	7.23	All	All	All
Application	Drupal	Drupal	7.3	All	All	All
Application	Drupal	Drupal	7.4	All	All	All
Application	Drupal	Drupal	7.5	All	All	All
Application	Drupal	Drupal	7.6	All	All	All
Application	Drupal	Drupal	7.7	All	All	All
Application	Drupal	Drupal	7.8	All	All	All
Application	Drupal	Drupal	7.9	All	All	All
Application	Drupal	Drupal	7.x-dev	All	All	All
cpe:2.3:a:drupal:drupal:7.0:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:alpha1:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:alpha2:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:alpha3:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:alpha4:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:alpha5:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:alpha6:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:alpha7:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:beta1:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:beta2:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:beta3:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:dev:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:rc1:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:rc2:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:rc3:*****:~:						
cpe:2.3:a:drupal:drupal:7.0:rc4:*****:~:						
cpe:2.3:a:drupal:drupal:7.1:*****:~:						

cpe:2.3:a:drupal:drupal:7.10:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.11:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.12:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.13:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.14:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.15:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.16:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.17:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.18:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.19:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.2:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.20:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.21:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.22:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.23:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.3:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.4:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.5:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.6:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.7:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.8:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.9:*:*:*:*:*:*:

```
cpe:2.3:a:drupal:drupal:7.x-dev:*:*:*:*:*:*:
```

cpe:2.3:a:drupal:drupal:7.0:*:*:*:*:*:*:

```
cpe:2.3:a:drupal:drupal:7.0:alpha1:*:*:*:*:*:
```

cpe:2.3:a:drupal:drupal:7.0:alpha2:*:*:*:*:*:

```
cpe:2.3:a:drupal:drupal:7.0:alpha3:*:*:*:*:*:
```

```
cpe:2.3:a:drupal:drupal:7.0:alpha4:*:*:*:*:*:
```

cpe:2.3:a:drupal:drupal:7.0:alpha5:*****:
cpe:2.3:a:drupal:drupal:7.0:alpha6:*****:
cpe:2.3:a:drupal:drupal:7.0:alpha7:*****:
cpe:2.3:a:drupal:drupal:7.0:beta1:*****:
cpe:2.3:a:drupal:drupal:7.0:beta2:*****:
cpe:2.3:a:drupal:drupal:7.0:beta3:*****:
cpe:2.3:a:drupal:drupal:7.0:dev:*****:
cpe:2.3:a:drupal:drupal:7.0:rc1:*****:
cpe:2.3:a:drupal:drupal:7.0:rc2:*****:
cpe:2.3:a:drupal:drupal:7.0:rc3:*****:
cpe:2.3:a:drupal:drupal:7.0:rc4:*****:
cpe:2.3:a:drupal:drupal:7.1:*****:
cpe:2.3:a:drupal:drupal:7.10:*****:
cpe:2.3:a:drupal:drupal:7.11:*****:
cpe:2.3:a:drupal:drupal:7.12:*****:
cpe:2.3:a:drupal:drupal:7.13:*****:
cpe:2.3:a:drupal:drupal:7.14:*****:
cpe:2.3:a:drupal:drupal:7.15:*****:
cpe:2.3:a:drupal:drupal:7.16:*****:
cpe:2.3:a:drupal:drupal:7.17:*****:
cpe:2.3:a:drupal:drupal:7.18:*****:
cpe:2.3:a:drupal:drupal:7.19:*****:
cpe:2.3:a:drupal:drupal:7.2:*****:
cpe:2.3:a:drupal:drupal:7.20:*****:
cpe:2.3:a:drupal:drupal:7.21:*****:
cpe:2.3:a:drupal:drupal:7.22:*****:
cpe:2.3:a:drupal:drupal:7.23:*****:
cpe:2.3:a:drupal:drupal:7.3:*****:
cpe:2.3:a:drupal:drupal:7.4:*****:

cpe:2.3:a:drupal:drupal:7.5:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.6:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.7:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.8:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.9:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.x-dev:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)