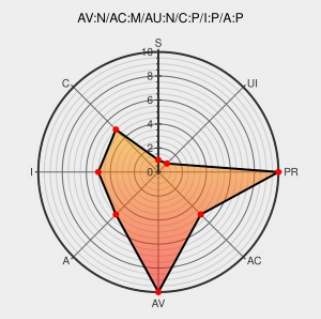
CVE-2008-6532

Published on: 03/26/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:17 PM UTC

CVE-2008-6532

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Drupal from Drupal contain the following vulnerability:

Multiple cross-site request forgery (CSRF) vulnerabilities in the update feature in Drupal 5.x before 5.13 and 6.x before 6.7 allow remote attackers to perform unauthorized actions as the superuser via unspecified vectors, as demonstrated by causing the superuser to "execute old updates" that modify the database.

CVE-2008-6532 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
[SECURITY] Fedora 8 Update: drupal-5.13-1.fc8	www.redhat.com, text/html	FEDORA FEDORA-2008-11196
[SECURITY] Fedora 9 Update: drupal-6.7-1.fc9	www.redhat.com, text/html	FEDORA FEDORA-2008-11213
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com, text/html	VUPEN ADV-2008-3414
SA-2008-073 - Drupal core - Multiple vulnerabilities | drupal.org	Patch, Vendor Advisory, drupal.org, text/html	CONFIRM drupal.org/node/345441
No Description Provided	www.osvdb.org	OSVDB 50661

	Inactive Link Not Archived	
Fedora update for drupal - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 33147
Drupal Cross-Site Request Forgery and Script Insertion - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 33112
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF drupal-unspecified-superuser-csrf(47260)

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	5.0	All	All	All
Application	Drupal	Drupal	5.1	All	All	All
Application	Drupal	Drupal	5.10	All	All	All
Application	Drupal	Drupal	5.11	All	All	All
Application	Drupal	Drupal	5.12	All	All	All
Application	Drupal	Drupal	5.2	All	All	All
Application	Drupal	Drupal	5.3	All	All	All
Application	Drupal	Drupal	5.4	All	All	All
Application	Drupal	Drupal	5.5	All	All	All
Application	Drupal	Drupal	5.6	All	All	All
Application	Drupal	Drupal	5.7	All	All	All
Application	Drupal	Drupal	5.8	All	All	All
Application	Drupal	Drupal	5.9	All	All	All
Application	Drupal	Drupal	6.0	All	All	All
Application	Drupal	Drupal	6.1	All	All	All
Application	Drupal	Drupal	6.2	All	All	All
Application	Drupal	Drupal	6.3	All	All	All
Application	Drupal	Drupal	6.4	All	All	All
Application	Drupal	Drupal	6.5	All	All	All
Application	Drupal	Drupal	6.6	All	All	All
Application	Drupal	Drupal	5.0	All	All	All

Application	Drupal	Drupal	5.1	All	All	All
Application	Drupal	Drupal	5.10	All	All	All
Application	Drupal	Drupal	5.11	All	All	All
Application	Drupal	Drupal	5.12	All	All	All
Application	Drupal	Drupal	5.2	All	All	All
Application	Drupal	Drupal	5.3	All	All	All
Application	Drupal	Drupal	5.4	All	All	All
Application	Drupal	Drupal	5.5	All	All	All
Application	Drupal	Drupal	5.6	All	All	All
Application	Drupal	Drupal	5.7	All	All	All
Application	Drupal	Drupal	5.8	All	All	All
Application	Drupal	Drupal	5.9	All	All	All
Application	Drupal	Drupal	6.0	All	All	All
Application	Drupal	Drupal	6.1	All	All	All
Application	Drupal	Drupal	6.2	All	All	All
Application	Drupal	Drupal	6.3	All	All	All
Application	Drupal	Drupal	6.4	All	All	All
Application	Drupal	Drupal	6.5	All	All	All
Application	Drupal	Drupal	6.6	All	All	All

cpe:2.3:a:drupal:drupal:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.1:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.10:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.11:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.12:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.2:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.3:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.4:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.5:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.6:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.7:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.8:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.9:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.1:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.2:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.3:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.4:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.5:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.6:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.1:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.10:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.11:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.12:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.2:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.3:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.4:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.5:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.6:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.7:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.8:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:5.9:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.1:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.2:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.3:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.4:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.5:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:6.6:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→