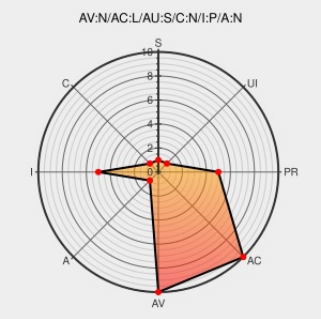
CVE-2005-3975

Published on: 12/03/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:23 PM UTC

CVE-2005-3975

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



Certain versions of Drupal from Drupal contain the following vulnerability:

Interpretation conflict in file.inc in Drupal 4.5.0 through 4.5.5 and 4.6.0 through 4.6.3 allows remote authenticated users to inject arbitrary web script or HTML via HTML in a file with a GIF or JPEG file extension, which causes the HTML to be executed by a victim who views the file in Internet Explorer as a result of CVE-2005-3312. NOTE: it could be argued that this vulnerability is due to a design flaw in Internet Explorer and the proper fix should be in that browser; if so, then this should not be treated as a vulnerability in Drupal.

CVE-2005-3975 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Secunia - Advisories - Debian update for drupal	web.archive.org text/html	SECUNIA 18630
Secunia - Advisories - Drupal Multiple Vulnerabilities	Patch Vendor Advisory web.archive.org text/html	SECUNIA 17824
	Patch Vendor Advisory drupal.org text/plain	CONFIRM drupal.org/files/sa-2005-008/advisory.txt

SecurityReason	securityreason.com text/html	SREASON 220
	drupal.org text/x-diff	MISC drupal.org/files/sa-2005-008/4.6.3.patch
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051201 [DRUPAL-SA-2005-008] Drupal 4.6.4 / 4.5.6 fixes XSS and HTTP header injection issue
Debian -- Security Information -- DSA-958-1 drupal	www.debian.org Depreciated Link text/html	DEBIAN DSA-958
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2005-2684
Drupal Image Upload HTML Injection Vulnerability	Patch cve.report (archive) text/html	BID 15663

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	4.5.0	All	All	All
Application	Drupal	Drupal	4.5.1	All	All	All
Application	Drupal	Drupal	4.5.2	All	All	All
Application	Drupal	Drupal	4.5.3	All	All	All
Application	Drupal	Drupal	4.5.4	All	All	All
Application	Drupal	Drupal	4.5.5	All	All	All
Application	Drupal	Drupal	4.6.0	All	All	All
Application	Drupal	Drupal	4.6.1	All	All	All
Application	Drupal	Drupal	4.6.2	All	All	All
Application	Drupal	Drupal	4.6.3	All	All	All
Application	Drupal	Drupal	4.5.0	All	All	All
Application	Drupal	Drupal	4.5.1	All	All	All
Application	Drupal	Drupal	4.5.2	All	All	All
Application	Drupal	Drupal	4.5.3	All	All	All
Application	Drupal	Drupal	4.5.4	All	All	All
Application	Drupal	Drupal	4.5.5	All	All	All
Application	Drupal	Drupal	4.6.0	All	All	All

Application	Drupal	Drupal	4.6.1	All	All	All
Application	Drupal	Drupal	4.6.2	All	All	All
Application	Drupal	Drupal	4.6.3	All	All	All

cpe:2.3:a:drupal:drupal:4.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.5.5:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.5.5:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:4.6.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report