

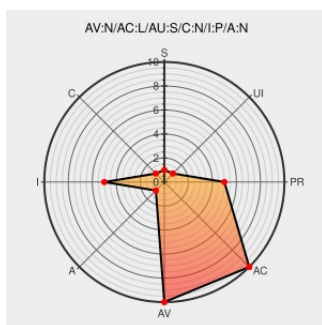


# CVE-2005-3975

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 [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access  
Vector

**NETWORK**

Access  
Complexity

**LOW**

Authentication

**SINGLE**

Confidentiality  
Impact

**NONE**

Integrity  
Impact

**PARTIAL**

Availability  
Impact

**NONE**

## CVE References

Description

Tags

Link

Secunia - Advisories - Debian update for drupal

[web.archive.org](#)  
[text/html](#)

[X SECUNIA 18630](#)

Secunia - Advisories - Drupal Multiple Vulnerabilities

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

[X SECUNIA 17824](#)

[CONFIRM drupal.org/files/sa-2005-008/advisory.txt](#)

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

|                                                                  |                                                                                                                                     |                                                                                                                                                                                                |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SecurityReason                                                   | <a href="https://securityreason.com/text/html">securityreason.com</a><br><a href="#">text/html</a>                                  |  SREASON 220                                                                                                  |
|                                                                  | <a href="https://drupal.org/text/x-diff">drupal.org</a><br><a href="#">text/x-diff</a>                                              |  MISC <a href="https://drupal.org/files/sa-2005-008/4.6.3.patch">drupal.org/files/sa-2005-008/4.6.3.patch</a> |
| SecurityFocus                                                    | <a href="https://www.securityfocus.com/text/html">www.securityfocus.com</a><br><a href="#">text/html</a>                            |  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               | <a href="https://www.debian.org/Deprecated Link">www.debian.org</a><br><a href="#">Deprecated Link</a><br><a href="#">text/html</a> |  DEBIAN DSA-958                                                                                               |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | <a href="https://www.vupen.com/text/html">www.vupen.com</a><br><a href="#">text/html</a>                                            |  VUPEN ADV-2005-2684                                                                                          |
| Drupal Image Upload HTML Injection Vulnerability                 | <a href="#">Patch</a><br><a href="#">cve.report (archive)</a><br><a href="#">text/html</a>                                          |  BID 15663                                                                                                    |

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](mailto: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 | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.5.0   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.5.1   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.5.2   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.5.3   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.5.4   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.5.5   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.6.0   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.6.1   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.6.2   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.6.3   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.5.0   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.5.1   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.5.2   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.5.3   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.5.4   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 4.5.5   | All    | All     | All      |
| Application | <a href="#">Drupal</a> | <a href="#">Drupal</a> | 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 →](#)

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](#)