



# CVE-2015-4393

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2015-4393                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | cve@mitre.org                                                                                                               |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2015-06-15 14:59:00 UTC                                                                                                     |
| <b>Updated</b>         | 2016-06-09 21:32:00 UTC                                                                                                     |
| <b>Description</b>     | The resource/endpoint for uploading files in the Services module 7.x-3.x before 7.x-3.12 for Drupal allows remote authentic |

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                           | Product                  | Version  | Update | Edition | Language |
|-------------|----------------------------------|--------------------------|----------|--------|---------|----------|
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.0  | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.1  | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.10 | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.11 | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.2  | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.3  | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.4  | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.5  | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.6  | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.7  | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.9  | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.0  | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.1  | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.10 | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.11 | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.2  | All    | All     | All      |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.3  | All    | All     | All      |

|             |                                  |                          |         |     |     |     |
|-------------|----------------------------------|--------------------------|---------|-----|-----|-----|
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.4 | All | All | All |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.5 | All | All | All |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.6 | All | All | All |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.7 | All | All | All |
| Application | <a href="#">Services Project</a> | <a href="#">Services</a> | 7.x-3.9 | All | All | All |

| References                                                                                                   |         |                         |
|--------------------------------------------------------------------------------------------------------------|---------|-------------------------|
| Reference                                                                                                    | Source  | Link                    |
| Drupal Services Module Access Bypass and Information Disclosure Vulnerabilities                              | BID     | <a href="#">www.se</a>  |
| services 7.x-3.12   Drupal.org                                                                               | CONFIRM | <a href="#">www.dr</a>  |
| oss-security - CVE requests for Drupal contributed modules (from SA-CONTRIB-2015-034 to SA-CONTRIB-2015-099) | MLIST   | <a href="#">www.ql</a>  |
| Services - Critical - Multiple Vulnerabilites - SA-CONTRIB-2015-096   Drupal.org                             | MISC    | <a href="#">www.dr</a>  |
| CVE Program record                                                                                           | CVE.ORG | <a href="#">www.cv</a>  |
| NVD vulnerability detail                                                                                     | NVD     | <a href="#">nvd.nis</a> |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.