



# CVE-2017-12794

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-12794                                                                                                             |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | cve@mitre.org                                                                                                              |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2017-09-07 13:29:00 UTC                                                                                                    |
| <b>Updated</b>         | 2018-03-16 01:29:00 UTC                                                                                                    |
| <b>Description</b>     | In Django 1.10.x before 1.10.8 and 1.11.x before 1.11.5, HTML autoescaping was disabled in a portion of the template for t |

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                        | Product                | Version | Update | Edition | Language |
|-------------|-------------------------------|------------------------|---------|--------|---------|----------|
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.0  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.1  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.2  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.3  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.4  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.5  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.6  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.7  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.11.0  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.11.1  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.11.2  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.11.3  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.11.4  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.0  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.1  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.2  | All    | All     | All      |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.3  | All    | All     | All      |

|             |                               |                        |        |     |     |     |
|-------------|-------------------------------|------------------------|--------|-----|-----|-----|
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.4 | All | All | All |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.5 | All | All | All |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.6 | All | All | All |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.10.7 | All | All | All |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.11.0 | All | All | All |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.11.1 | All | All | All |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.11.2 | All | All | All |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.11.3 | All | All | All |
| Application | <a href="#">Djangoproject</a> | <a href="#">Django</a> | 1.11.4 | All | All | All |

## References

| Reference                                                                                                                       | Source |
|---------------------------------------------------------------------------------------------------------------------------------|--------|
| Django Input Validation Flaw in Technical 500 Template Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker | SECTR  |
| Django security releases issued: 1.11.5 and 1.10.8   Weblog   Django                                                            | CONFII |
| USN-3559-1: Django vulnerabilities   Ubuntu security notices                                                                    | UBUNT  |
| Django CVE-2017-12794 Cross Site Scripting Vulnerability                                                                        | BID    |
| CVE Program record                                                                                                              | CVE.OI |
| NVD vulnerability detail                                                                                                        | NVD    |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

|                                                                                      |
|--------------------------------------------------------------------------------------|
| <a href="#">500580</a> Alpine Linux Security Update for py3-django                   |
| <a href="#">981145</a> Python (pip) Security Update for django (GHSA-9r8w-6x8c-6jr9) |