



# CVE-2013-0306

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

## Summary

|                 |                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2013-0306                                                                                                                 |
| State           | PUBLISHED                                                                                                                     |
| Assigner        | redhat                                                                                                                        |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                  |
| Published       | 2013-05-02 14:55:05 UTC                                                                                                       |
| Updated         | 2026-04-29 01:13:23 UTC                                                                                                       |
| Description     | The form library in Django 1.3.x before 1.3.6, 1.4.x before 1.4.4, and 1.5 before release candidate 2 allows remote attackers |

## Risk And Classification

**Primary CVSS:** v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

**Problem Types:** CWE-189 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor    | Product      | Version | Update | Edition | Language |
|------------------|-----------|--------------|---------|--------|---------|----------|
| Operating System | Canonical | Ubuntu Linux | 10.04   | -      | lts     | All      |

|                  |                               |                              |       |        |     |     |
|------------------|-------------------------------|------------------------------|-------|--------|-----|-----|
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 11.10 | All    | All | All |
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 12.04 | -      | Its | All |
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 12.10 | All    | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.3   | All    | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.3   | alpha1 | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.3   | beta1  | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.3.1 | All    | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.3.2 | All    | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.3.3 | All    | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.4   | All    | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.4   | alpha  | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.4   | beta   | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.4.1 | All    | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.4.2 | All    | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.5   | alpha  | All | All |
| Application      | <a href="#">Djangoproject</a> | <a href="#">Django</a>       | 1.5   | beta   | All | All |

| Vendor Declared Affected Products |                    |                     |              |               |  |
|-----------------------------------|--------------------|---------------------|--------------|---------------|--|
| Source                            | Vendor             | Product             | Version      | Platforms     |  |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |  |

| References                                                 |                                      |  |                                       |        |
|------------------------------------------------------------|--------------------------------------|--|---------------------------------------|--------|
| Reference                                                  | Source                               |  | Link                                  | Tags   |
| Debian -- Security Information -- DSA-2634-1 python-django | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">www.debian.org</a>        |        |
| Red Hat Customer Portal                                    | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">rhn.redhat.com</a>        |        |
| USN-1757-1: Django vulnerabilities   Ubuntu                | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">ubuntu.com</a>            |        |
| Security releases issued   Weblog   Django                 | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">www.djangoproject.com</a> | Vendo  |
| CVE Program record                                         | CVE.ORG                              |  | <a href="#">www.cve.org</a>           | canoni |
| NVD vulnerability detail                                   | NVD                                  |  | <a href="#">nvd.nist.gov</a>          | canoni |

No vendor comments have been submitted for this CVE.

| Legacy QID Mappings                                                                  |
|--------------------------------------------------------------------------------------|
| <a href="#">994972</a> Python (Pip) Security Update for django (GHSA-g8xg-jgj6-49r3) |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)