



CVE-2015-0222

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

Summary

CVE	CVE-2015-0222
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-16 16:59:21 UTC
Updated	2026-05-06 22:30:45 UTC
Description	ModelMultipleChoiceField in Django 1.6.x before 1.6.10 and 1.7.x before 1.7.3, when show_hidden_initial is set to True, all

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-17 | 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	All	Its	All

Operating System	Canonical	Ubuntu Linux	12.04	All	Its	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Application	Djangoproject	Django	1.6	All	All	All
Application	Djangoproject	Django	1.6.1	All	All	All
Application	Djangoproject	Django	1.6.2	All	All	All
Application	Djangoproject	Django	1.6.3	All	All	All
Application	Djangoproject	Django	1.6.4	All	All	All
Application	Djangoproject	Django	1.6.5	All	All	All
Application	Djangoproject	Django	1.6.6	All	All	All
Application	Djangoproject	Django	1.6.7	All	All	All
Application	Djangoproject	Django	1.6.8	All	All	All
Application	Djangoproject	Django	1.6.9	All	All	All
Application	Djangoproject	Django	1.7	All	All	All
Application	Djangoproject	Django	1.7.1	All	All	All
Application	Djangoproject	Django	1.7.2	All	All	All
Application	Djangoproject	Django	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
[SECURITY] Fedora 20 Update: python-django-1.6.10-1.fc20	af854a3a-2127-42d1-9000-000000000000
[SECURITY] Fedora 20 Update: python-django14-1.4.18-1.fc20	af854a3a-2127-42d1-9000-000000000000
[SECURITY] Fedora 21 Update: python-django-1.6.10-1.fc21	af854a3a-2127-42d1-9000-000000000000
Mageia Advisory: MGASA-2015-0026 - Updated python-django and python-django14 packages fix security vulnerabilities	af854a3a-2127-42d1-9000-000000000000
Security Advisory SA62285 - Ubuntu update for django - Secunia	af854a3a-2127-42d1-9000-000000000000
openSUSE-SU-2015:0643-1: moderate: Security update for python-Django	af854a3a-2127-42d1-9000-000000000000
USN-2469-1: Django vulnerabilities Ubuntu	af854a3a-2127-42d1-9000-000000000000
Security releases issued Weblog Django	af854a3a-2127-42d1-9000-000000000000
Security Advisory SA62309 - Django Cross-Site Scripting and Denial of Service Vulnerabilities - Secunia	af854a3a-2127-42d1-9000-000000000000
openSUSE-SU-2015:1598-1: moderate: Security update for python-django	af854a3a-2127-42d1-9000-000000000000
Support / Security / Advisories // MDVSA-2015:109 Mandriva	af854a3a-2127-42d1-9000-000000000000
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)