



CVE-2014-3730

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

Summary

CVE	CVE-2014-3730
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-16 15:55:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	The django.util.http.is_safe_url function in Django 1.4 before 1.4.13, 1.5 before 1.5.8, 1.6 before 1.6.5, and 1.7 before 1.7b4

Risk And Classification

Problem Types: CWE-20

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	Canonical	Ubuntu Linux	12.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Djangoproject	Django	1.4	All	All	All
Application	Djangoproject	Django	1.4.1	All	All	All
Application	Djangoproject	Django	1.4.10	All	All	All

Django versions						
Application	Djangoproject	Django	1.4.11	All	All	All
Application	Djangoproject	Django	1.4.12	All	All	All
Application	Djangoproject	Django	1.4.2	All	All	All
Application	Djangoproject	Django	1.4.4	All	All	All
Application	Djangoproject	Django	1.4.5	All	All	All
Application	Djangoproject	Django	1.4.6	All	All	All
Application	Djangoproject	Django	1.4.7	All	All	All
Application	Djangoproject	Django	1.4.8	All	All	All
Application	Djangoproject	Django	1.4.9	All	All	All
Application	Djangoproject	Django	1.5	All	All	All
Application	Djangoproject	Django	1.5	alpha	All	All
Application	Djangoproject	Django	1.5	beta	All	All
Application	Djangoproject	Django	1.5.1	All	All	All
Application	Djangoproject	Django	1.5.2	All	All	All
Application	Djangoproject	Django	1.5.3	All	All	All
Application	Djangoproject	Django	1.5.4	All	All	All
Application	Djangoproject	Django	1.5.5	All	All	All
Application	Djangoproject	Django	1.5.6	All	All	All
Application	Djangoproject	Django	1.5.7	All	All	All
Application	Djangoproject	Django	1.6	-	All	All
Application	Djangoproject	Django	1.6	beta1	All	All
Application	Djangoproject	Django	1.6	beta2	All	All
Application	Djangoproject	Django	1.6	beta3	All	All
Application	Djangoproject	Django	1.6	beta4	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	1.7	beta1	All	All
Application	Djangoproject	Django	1.7	beta2	All	All
Application	Djangoproject	Django	1.7	beta3	All	All
Application	Djangoproject	Django	1.4	All	All	All
Application	Djangoproject	Django	1.4.1	All	All	All
Application	Djangoproject	Django	1.4.10	All	All	All
Application	Djangoproject	Django	1.4.11	All	All	All

Application	Djangoproject	Django	1.4.12	All	All	All
Application	Djangoproject	Django	1.4.2	All	All	All
Application	Djangoproject	Django	1.4.4	All	All	All
Application	Djangoproject	Django	1.4.5	All	All	All
Application	Djangoproject	Django	1.4.6	All	All	All
Application	Djangoproject	Django	1.4.7	All	All	All
Application	Djangoproject	Django	1.4.8	All	All	All
Application	Djangoproject	Django	1.4.9	All	All	All
Application	Djangoproject	Django	1.5	All	All	All
Application	Djangoproject	Django	1.5	alpha	All	All
Application	Djangoproject	Django	1.5	beta	All	All
Application	Djangoproject	Django	1.5.1	All	All	All
Application	Djangoproject	Django	1.5.2	All	All	All
Application	Djangoproject	Django	1.5.3	All	All	All
Application	Djangoproject	Django	1.5.4	All	All	All
Application	Djangoproject	Django	1.5.5	All	All	All
Application	Djangoproject	Django	1.5.6	All	All	All
Application	Djangoproject	Django	1.5.7	All	All	All
Application	Djangoproject	Django	1.6	-	All	All
Application	Djangoproject	Django	1.6	beta1	All	All
Application	Djangoproject	Django	1.6	beta2	All	All
Application	Djangoproject	Django	1.6	beta3	All	All
Application	Djangoproject	Django	1.6	beta4	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	1.7	beta1	All	All
Application	Djangoproject	Django	1.7	beta2	All	All
Application	Djangoproject	Django	1.7	beta3	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All

Reference	Source	Link	Tags
oss-security - Re: CVE Reuest: Django: Malformed URLs from user input incorrectly validated	MLIST	www.openwall.com	Third
Debian -- Security Information -- DSA-2934-1 python-django	DEBIAN	www.debian.org	Third
Django 'is_safe_url()' Function URI Redirection Vulnerability	BID	www.securityfocus.com	Third
USN-2212-1: Django vulnerabilities Ubuntu	UBUNTU	ubuntu.com	Third
Security Advisory SA61281 - SUSE update for python-django - Secunia	SECUNIA	secunia.com	
oss-security - CVE Reuest: Django: Malformed URLs from user input incorrectly validated	MLIST	www.openwall.com	Third
Security releases issued Weblog Django	CONFIRM	www.djangoproject.com	Patch
openSUSE-SU-2014:1132-1: moderate: python-django: security and bugfix up	SUSE	lists.opensuse.org	Third
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor
No vendor comments have been submitted for this CVE.			
Legacy QID Mappings			
994933 Python (Pip) Security Update for django (GHSA-vq3h-3q7v-9prw)			

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report