



CVE-2015-5143

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

Summary

CVE	CVE-2015-5143
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-14 17:59:00 UTC
Updated	2017-09-22 01:29:00 UTC
Description	The session backends in Django before 1.4.21, 1.5.x through 1.6.x, 1.7.x before 1.7.9, and 1.8.x before 1.8.3 allows remote

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	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	1.4.20	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

Django versions						
Application	Djangoproject	Django	1.5.10	All	All	All
Application	Djangoproject	Django	1.5.11	All	All	All
Application	Djangoproject	Django	1.5.12	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	1.5.8	All	All	All
Application	Djangoproject	Django	1.5.9	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	1.6.10	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	beta1	All	All
Application	Djangoproject	Django	1.7	beta2	All	All
Application	Djangoproject	Django	1.7	beta3	All	All
Application	Djangoproject	Django	1.7	beta4	All	All
Application	Djangoproject	Django	1.7	rc1	All	All
Application	Djangoproject	Django	1.7	rc2	All	All
Application	Djangoproject	Django	1.7	rc3	All	All
Application	Djangoproject	Django	1.7.1	All	All	All
Application	Djangoproject	Django	1.7.2	All	All	All

Application	Djangoproject	Django	1.7.3	All	All	All
Application	Djangoproject	Django	1.7.4	All	All	All
Application	Djangoproject	Django	1.7.5	All	All	All
Application	Djangoproject	Django	1.7.6	All	All	All
Application	Djangoproject	Django	1.7.7	All	All	All
Application	Djangoproject	Django	1.7.8	All	All	All
Application	Djangoproject	Django	1.7.9	All	All	All
Application	Djangoproject	Django	1.8.0	All	All	All
Application	Djangoproject	Django	1.8.1	All	All	All
Application	Djangoproject	Django	1.8.2	All	All	All
Application	Djangoproject	Django	1.4.20	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	1.5.10	All	All	All
Application	Djangoproject	Django	1.5.11	All	All	All
Application	Djangoproject	Django	1.5.12	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	1.5.8	All	All	All
Application	Djangoproject	Django	1.5.9	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	1.6.10	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	1.6.4	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	beta1	All	All
Application	Djangoproject	Django	1.7	beta2	All	All
Application	Djangoproject	Django	1.7	beta3	All	All
Application	Djangoproject	Django	1.7	beta4	All	All
Application	Djangoproject	Django	1.7	rc1	All	All
Application	Djangoproject	Django	1.7	rc2	All	All
Application	Djangoproject	Django	1.7	rc3	All	All
Application	Djangoproject	Django	1.7.1	All	All	All
Application	Djangoproject	Django	1.7.2	All	All	All
Application	Djangoproject	Django	1.7.3	All	All	All
Application	Djangoproject	Django	1.7.4	All	All	All
Application	Djangoproject	Django	1.7.5	All	All	All
Application	Djangoproject	Django	1.7.6	All	All	All
Application	Djangoproject	Django	1.7.7	All	All	All
Application	Djangoproject	Django	1.7.8	All	All	All
Application	Djangoproject	Django	1.7.9	All	All	All
Application	Djangoproject	Django	1.8.0	All	All	All
Application	Djangoproject	Django	1.8.1	All	All	All
Application	Djangoproject	Django	1.8.2	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All

References						
Reference					Source	Link
Red Hat Customer Portal					REDHAT	rhn.r
Django: Multiple vulnerabilities (GLSA 201510-06) — Gentoo Security					GENTOO	secu
Oracle Solaris Third Party Bulletin - October 2015					CONFIRM	www
[SECURITY] Fedora 23 Update: python-django-1.8.6-1.fc23					FEDORA	lists.
Red Hat Customer Portal					REDHAT	rhn.r
Debian -- Security Information -- DSA-3305-1 python-django					DEBIAN	www

openSUSE-SU-2015:1813-1: moderate: Security update for python-Django	SUSE	lists.
Django Bugs Let Remote Users Deny Service and Conduct HTTP/Header Response Splitting Attacks - SecurityTracker	SECTrack	www
openSUSE-SU-2015:1802-1: moderate: Security update for python-django	SUSE	lists.
Security releases issued: 1.8.3, 1.7.9, 1.4.21 Weblog Django	CONFIRM	www
Django CVE-2015-5143 Denial of Service Vulnerability	BID	www
USN-2671-1: Django vulnerabilities Ubuntu	UBUNTU	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.i

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981068](#) Python (pip) Security Update for django (GHSA-h582-2pch-3xv3)

© [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](#)