



CVE-2014-0473

Published on: 04/23/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:56 PM UTC

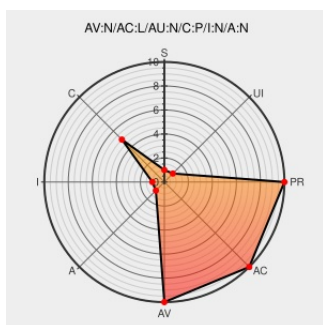
CVE-2014-0473

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

The caching framework in Django before 1.4.11, 1.5.x before 1.5.6, 1.6.x before 1.6.3, and 1.7.x before 1.7 beta 2 reuses a cached CSRF token for all anonymous users, which allows remote attackers to bypass CSRF protections by reading the CSRF cookie for anonymous users.

CVE-2014-0473 has been assigned by security@debian.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

Security releases issued | Weblog | Django

[Vendor Advisory](#)
[www.djangoproject.com](#)
[text/html](#)

CONFIRM
[www.djangoproject.com/weblog/2014/apr/21/security/](#)

Debian -- Security Information -- DSA-2934-1 python-django

[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

DEBIAN DSA-2934

Red Hat Customer Portal

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

REDHAT RHSA-2014:0457

Security Advisory SA61281 - SUSE update for python-django - Secunia

[web.archive.org](#)
[text/html](#)

SECUNIA 61281

USN-2169-1: Django vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2169-1
openSUSE-SU-2014:1132-1: moderate: python-django: security and bugfix up	lists.opensuse.org text/html	 SUSE openSUSE-SU-2014:1132
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2014:0456

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	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	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	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
Application	Djangoproject	Django	1.4	All	All	All
Application	Djangoproject	Django	1.4.1	All	All	All
Application	Djangoproject	Django	1.4.2	All	All	All
Application	Djangoproject	Django	1.4.3	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	1.5.1	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	1.6	All	All	All
Application	Djangoproject	Django	1.6.1	All	All	All
Application	Djangoproject	Django	1.6.2	All	All	All
Application	Djangoproject	Django	1.7	alpha1	All	All
Application	Djangoproject	Django	1.7	alpha2	All	All
Application	Djangoproject	Django	1.7	beta1	All	All
Application	Djangoproject	Django	1.4	All	All	All
Application	Djangoproject	Django	1.4.1	All	All	All
Application	Djangoproject	Django	1.4.2	All	All	All
Application	Djangoproject	Django	1.4.3	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	1.5.1	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	1.6	All	All	All
Application	Djangoproject	Django	1.6.1	All	All	All
Application	Djangoproject	Django	1.6.2	All	All	All
Application	Djangoproject	Django	1.7	alpha1	All	All
Application	Djangoproject	Django	1.7	alpha2	All	All

Application	Djangoproject	Django	1.7	beta1	All	All
Application	Djangoproject	Django	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:~::~~::~~::~~::						
cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:~::~~::~~::~~::						
cpe:2.3:o:canonical:ubuntu_linux:12.10:~::~~::~~::~~::~~::						
cpe:2.3:o:canonical:ubuntu_linux:13.10:~::~~::~~::~~::~~::						
cpe:2.3:o:canonical:ubuntu_linux:14.04:~::~~::~~::~~::						
cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:~::~~::~~::~~::						
cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:~::~~::~~::~~::						
cpe:2.3:o:canonical:ubuntu_linux:12.10:~::~~::~~::~~::~~::						
cpe:2.3:o:canonical:ubuntu_linux:13.10:~::~~::~~::~~::~~::						
cpe:2.3:o:canonical:ubuntu_linux:14.04:~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.4:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.4.1:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.4.2:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.4.3:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.4.4:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.4.5:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.4.6:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.4.7:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.4.8:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.4.9:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.5:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.5.1:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.5.2:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.5.3:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.5.4:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.5.5:~::~~::~~::~~::~~::						
cpe:2.3:a:djangoproject:django:1.6:~::~~::~~::~~::~~::						

cpe:2.3:a:djangoproject:django:1.6.1:****:*:*:
cpe:2.3:a:djangoproject:django:1.6.2:****:*:*:
cpe:2.3:a:djangoproject:django:1.7:alpha1:****:*:*:
cpe:2.3:a:djangoproject:django:1.7:alpha2:****:*:*:
cpe:2.3:a:djangoproject:django:1.7:beta1:****:*:*:
cpe:2.3:a:djangoproject:django:1.4:****:*:*:
cpe:2.3:a:djangoproject:django:1.4.1:****:*:*:
cpe:2.3:a:djangoproject:django:1.4.2:****:*:*:
cpe:2.3:a:djangoproject:django:1.4.3:****:*:*:
cpe:2.3:a:djangoproject:django:1.4.4:****:*:*:
cpe:2.3:a:djangoproject:django:1.4.5:****:*:*:
cpe:2.3:a:djangoproject:django:1.4.6:****:*:*:
cpe:2.3:a:djangoproject:django:1.4.7:****:*:*:
cpe:2.3:a:djangoproject:django:1.4.8:****:*:*:
cpe:2.3:a:djangoproject:django:1.4.9:****:*:*:
cpe:2.3:a:djangoproject:django:1.5:****:*:*:
cpe:2.3:a:djangoproject:django:1.5.1:****:*:*:
cpe:2.3:a:djangoproject:django:1.5.2:****:*:*:
cpe:2.3:a:djangoproject:django:1.5.3:****:*:*:
cpe:2.3:a:djangoproject:django:1.5.4:****:*:*:
cpe:2.3:a:djangoproject:django:1.5.5:****:*:*:
cpe:2.3:a:djangoproject:django:1.6:****:*:*:
cpe:2.3:a:djangoproject:django:1.6.1:****:*:*:
cpe:2.3:a:djangoproject:django:1.6.2:****:*:*:
cpe:2.3:a:djangoproject:django:1.7:alpha1:****:*:*:
cpe:2.3:a:djangoproject:django:1.7:alpha2:****:*:*:
cpe:2.3:a:djangoproject:django:1.7:beta1:****:*:*:
cpe:2.3:a:djangoproject:django:****:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023  |

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](#).

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