



CVE-2016-9014

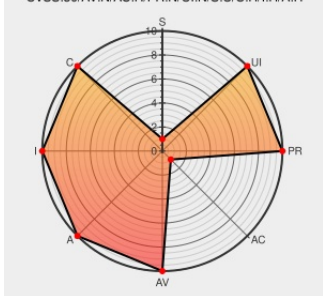
Published on: 12/09/2016 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:36:00 AM UTC

CVE-2016-9014

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H



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

Django before 1.8.x before 1.8.16, 1.9.x before 1.9.11, and 1.10.x before 1.10.3, when settings.DEBUG is True, allow remote attackers to conduct DNS rebinding attacks by leveraging failure to validate the HTTP Host header against settings.ALLOWED_HOSTS.

CVE-2016-9014 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] Fedora 25 Update: python-django-1.9.11-1.fc25 - package-announce - Fedora Mailing-Lists	Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2016-d4571bf555
[SECURITY] Fedora 24 Update: python-django-1.9.11-	lists.fedoraproject.org	FEDORA FEDORA-2016-3eb5a55123

1.fc24 - package-announce - Fedora Mailing-Lists	text/html	
Django Bugs Let Remote Users Access the Database in Certain Cases, Conduct Cross-Site Scripting Attacks, and Obtain Potentially Sensitive Information - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTrack 1037159
Debian -- Security Information -- DSA-3835-1 python-django	www.debian.org Depreciated Link text/html	DEBIAN DSA-3835
USN-3115-1: Django vulnerabilities Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-3115-1
Django security releases issued: 1.10.3, 1.9.11 and 1.8.16 Weblog Django	Release Notes Vendor Advisory www.djangoproject.com text/html	CONFIRM www.djangoproject.com/weblog/2016/nov/01/security-releases/
Django CVE-2016-9014 Security Bypass Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	CVE BID 94068

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.

Related QID Numbers

[500581](#) Alpine Linux Security Update for py3-django

Known Affected Configurations (CPE V2.3)

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	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.10	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	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.10	All	All	All
Application	Djangoproject	Django	1.10	All	All	All
Application	Djangoproject	Django	1.10.1	All	All	All

Application	Djangoproject	Django	Python	OS	License	Website
Application	Djangoproject	Django	1.10.2	All	All	All
Application	Djangoproject	Django	1.8	All	All	All
Application	Djangoproject	Django	1.8.1	All	All	All
Application	Djangoproject	Django	1.8.10	All	All	All
Application	Djangoproject	Django	1.8.11	All	All	All
Application	Djangoproject	Django	1.8.12	All	All	All
Application	Djangoproject	Django	1.8.13	All	All	All
Application	Djangoproject	Django	1.8.14	All	All	All
Application	Djangoproject	Django	1.8.15	All	All	All
Application	Djangoproject	Django	1.8.2	All	All	All
Application	Djangoproject	Django	1.8.3	All	All	All
Application	Djangoproject	Django	1.8.4	All	All	All
Application	Djangoproject	Django	1.8.5	All	All	All
Application	Djangoproject	Django	1.8.6	All	All	All
Application	Djangoproject	Django	1.8.7	All	All	All
Application	Djangoproject	Django	1.8.8	All	All	All
Application	Djangoproject	Django	1.8.9	All	All	All
Application	Djangoproject	Django	1.9	All	All	All
Application	Djangoproject	Django	1.9.1	All	All	All
Application	Djangoproject	Django	1.9.10	All	All	All
Application	Djangoproject	Django	1.9.2	All	All	All
Application	Djangoproject	Django	1.9.3	All	All	All
Application	Djangoproject	Django	1.9.4	All	All	All
Application	Djangoproject	Django	1.9.5	All	All	All
Application	Djangoproject	Django	1.9.6	All	All	All
Application	Djangoproject	Django	1.9.7	All	All	All
Application	Djangoproject	Django	1.9.8	All	All	All
Application	Djangoproject	Django	1.9.9	All	All	All
Application	Djangoproject	Django	1.10	All	All	All
Application	Djangoproject	Django	1.10.1	All	All	All
Application	Djangoproject	Django	1.10.2	All	All	All
Application	Djangoproject	Django	1.8	All	All	All
Application	Djangoproject	Django	1.8.1	All	All	All
Application	Djangoproject	Django	1.8.10	All	All	All
Application	Djangoproject	Django	1.8.11	All	All	All

Application	Djangoproject	Django	1.8.12	All	All	All
Application	Djangoproject	Django	1.8.13	All	All	All
Application	Djangoproject	Django	1.8.14	All	All	All
Application	Djangoproject	Django	1.8.15	All	All	All
Application	Djangoproject	Django	1.8.2	All	All	All
Application	Djangoproject	Django	1.8.3	All	All	All
Application	Djangoproject	Django	1.8.4	All	All	All
Application	Djangoproject	Django	1.8.5	All	All	All
Application	Djangoproject	Django	1.8.6	All	All	All
Application	Djangoproject	Django	1.8.7	All	All	All
Application	Djangoproject	Django	1.8.8	All	All	All
Application	Djangoproject	Django	1.8.9	All	All	All
Application	Djangoproject	Django	1.9	All	All	All
Application	Djangoproject	Django	1.9.1	All	All	All
Application	Djangoproject	Django	1.9.10	All	All	All
Application	Djangoproject	Django	1.9.2	All	All	All
Application	Djangoproject	Django	1.9.3	All	All	All
Application	Djangoproject	Django	1.9.4	All	All	All
Application	Djangoproject	Django	1.9.5	All	All	All
Application	Djangoproject	Django	1.9.6	All	All	All
Application	Djangoproject	Django	1.9.7	All	All	All
Application	Djangoproject	Django	1.9.8	All	All	All
Application	Djangoproject	Django	1.9.9	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	25	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	25	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:16.10:*****:***:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:lts:***:						

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:*:*:*:
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:*:*:*:
cpe:2.3:o:canonical:ubuntu_linux:16.10:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.10:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.10.1:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.10.2:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.1:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.10:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.11:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.12:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.13:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.14:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.15:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.2:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.3:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.4:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.5:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.6:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.7:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.8:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.8.9:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.9:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.9.1:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.9.10:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.9.2:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.9.3:*:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.9.4:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.9.5:*****:
cpe:2.3:a:djangoproject:django:1.9.6:*****:
cpe:2.3:a:djangoproject:django:1.9.7:*****:
cpe:2.3:a:djangoproject:django:1.9.8:*****:
cpe:2.3:a:djangoproject:django:1.9.9:*****:
cpe:2.3:a:djangoproject:django:1.10:*****:
cpe:2.3:a:djangoproject:django:1.10.1:*****:
cpe:2.3:a:djangoproject:django:1.10.2:*****:
cpe:2.3:a:djangoproject:django:1.8:*****:
cpe:2.3:a:djangoproject:django:1.8.1:*****:
cpe:2.3:a:djangoproject:django:1.8.10:*****:
cpe:2.3:a:djangoproject:django:1.8.11:*****:
cpe:2.3:a:djangoproject:django:1.8.12:*****:
cpe:2.3:a:djangoproject:django:1.8.13:*****:
cpe:2.3:a:djangoproject:django:1.8.14:*****:
cpe:2.3:a:djangoproject:django:1.8.15:*****:
cpe:2.3:a:djangoproject:django:1.8.2:*****:
cpe:2.3:a:djangoproject:django:1.8.3:*****:
cpe:2.3:a:djangoproject:django:1.8.4:*****:
cpe:2.3:a:djangoproject:django:1.8.5:*****:
cpe:2.3:a:djangoproject:django:1.8.6:*****:
cpe:2.3:a:djangoproject:django:1.8.7:*****:
cpe:2.3:a:djangoproject:django:1.8.8:*****:
cpe:2.3:a:djangoproject:django:1.8.9:*****:
cpe:2.3:a:djangoproject:django:1.9:*****:
cpe:2.3:a:djangoproject:django:1.9.1:*****:
cpe:2.3:a:djangoproject:django:1.9.10:*****:
cpe:2.3:a:djangoproject:django:1.9.2:*****:
cpe:2.3:a:djangoproject:django:1.9.3:*****:

cpe:2.3:a:djangoproject:django:1.9.4:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.9.5:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.9.6:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.9.7:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.9.8:*:*:*:*:*:
cpe:2.3:a:djangoproject:django:1.9.9:*:*:*:*:*:
cpe:2.3:o:fedoraproject:fedora:24:*:*:*:*:*:
cpe:2.3:o:fedoraproject:fedora:25:*:*:*:*:*:
cpe:2.3:o:fedoraproject:fedora:24:*:*:*:*:*:
cpe:2.3:o:fedoraproject:fedora:25:*:*:*:*:*:

```
cpe:2.3:o:fedoraproject:fedora:25:*:*:*:*:*:*:
```

Next ID→

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