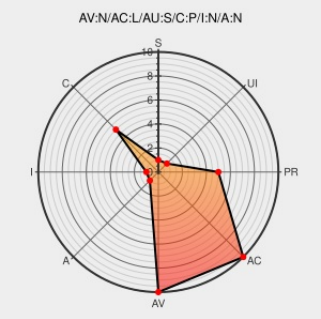
CVE-2013-0305

Published on: 05/02/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:14 AM UTC

CVE-2013-0305

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The administrative interface for Django 1.3.x before 1.3.6, 1.4.x before 1.4.4, and 1.5 before release candidate 2 does not check permissions for the history view, which allows remote authenticated administrators to obtain sensitive object history information.

CVE-2013-0305 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-2634-1 python-django	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-2634
Red Hat Customer Portal	web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2013:0670
USN-1757-1: Django vulnerabilities | Ubuntu	ubuntu.com, text/html	UBUNTU USN-1757-1
Security releases issued | Weblog | Django	Patch, Vendor Advisory, www.djangoproject.com, text/html	CONFIRM www.djangoproject.com/weblog/2013/feb/19/security/

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

994971 Python (Pip) Security Update for django (GHSA-r7w6-p47g-vj53)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	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	10.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Application	Djangoproject	Django	1.3	All	All	All
Application	Djangoproject	Django	1.3	alpha1	All	All
Application	Djangoproject	Django	1.3	beta1	All	All
Application	Djangoproject	Django	1.3.1	All	All	All
Application	Djangoproject	Django	1.3.2	All	All	All
Application	Djangoproject	Django	1.3.3	All	All	All
Application	Djangoproject	Django	1.4	All	All	All
Application	Djangoproject	Django	1.4	alpha	All	All
Application	Djangoproject	Django	1.4	beta	All	All
Application	Djangoproject	Django	1.4.1	All	All	All
Application	Djangoproject	Django	1.4.2	All	All	All
Application	Djangoproject	Django	1.5	alpha	All	All
Application	Djangoproject	Django	1.5	beta	All	All
Application	Djangoproject	Django	1.3	All	All	All
Application	Djangoproject	Django	1.3	alpha1	All	All

Application	Djangoproject	Django	1.3	beta1	All	All
Application	Djangoproject	Django	1.3.1	All	All	All
Application	Djangoproject	Django	1.3.2	All	All	All
Application	Djangoproject	Django	1.3.3	All	All	All
Application	Djangoproject	Django	1.4	All	All	All
Application	Djangoproject	Django	1.4	alpha	All	All
Application	Djangoproject	Django	1.4	beta	All	All
Application	Djangoproject	Django	1.4.1	All	All	All
Application	Djangoproject	Django	1.4.2	All	All	All
Application	Djangoproject	Django	1.5	alpha	All	All
Application	Djangoproject	Django	1.5	beta	All	All

cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:11.10:*:*:*:*:*:*:*:

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:10.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:11.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.3:alpha1:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.3:beta1:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.4:alpha:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.4:beta:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.5:alpha:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.5:beta:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.3:alpha1:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.3:beta1:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.4:alpha:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.4:beta:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.5:alpha:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.5:beta:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→