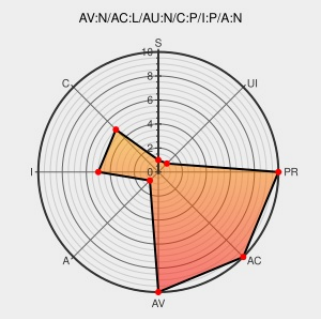
CVE-2012-4520

Published on: 11/18/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:15 PM UTC

CVE-2012-4520

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



Certain versions of Django from Djangoproject contain the following vulnerability:

The django.http.HttpRequest.get_host function in Django 1.3.x before 1.3.4 and 1.4.x before 1.4.2 allows remote attackers to generate and display arbitrary URLs via crafted username and password Host header values.

CVE-2012-4520 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
USN-1632-1: Django vulnerability | Ubuntu	ubuntu.com text/html	UBUNTU USN-1632-1
[SECURITY] Fedora 18 Update: python-django-1.4.2-1.fc18	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-16406
Fixed a security issue related to password resets · django/django@9305c0e · GitHub	github.com text/html	CONFIRM github.com/django/django/commit/9305c0e12d43c4df999c3301a1f0c742264a657e
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 86493

About Secunia Research | Flexera	Vendor Advisory secunia.com Depreciated Link text/plain	SECUNIA 51033
Fixed a security issue related to password resets · django/django@b45c377 · GitHub	github.com text/html	CONFIRM github.com/django/django/commit/b45c377f8f488955e0c7069cad3f3dd21910b071
Debian -- Security Information -- DSA-2634-1 python-django	www.debian.org Depreciated Link text/html	DEBIAN DSA-2634
865164 – (CVE-2012-4520) CVE-2012-4520 Django: Host header poisoning vulnerability	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=865164
About Secunia Research | Flexera	Vendor Advisory secunia.com Depreciated Link text/plain	SECUNIA 51314
[SECURITY] Fedora 16 Update: Django-1.3.4-1.fc16	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-16417
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/2012/oct/17/security/
oss-security - Re: CVE Request: Django	www.openwall.com text/html	MLIST [oss-security] 20121029 Re: CVE Request: Django
Django Host Header Filtering Bug Lets Remote Users Cuase Arbitrary URLs to be Displayed - SecurityTracker	securitytracker.com text/html	SECTRACK 1027708
[SECURITY] Fedora 17 Update: Django-1.4.2-1.fc17	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-16440
#691145 - python-django: CVE-2012-4520 - Debian Bug report logs	bugs.debian.org text/html	MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=691145
Fixed a security issue related to password resets · django/django@92d3430 · GitHub	github.com text/html	CONFIRM github.com/django/django/commit/92d3430f12171f16f566c9050c40feefb830a4a3

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.4.1	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	1.4.1	All	All	All

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:1.4.1:*:*:*:*:*:*:*:

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:1.4.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→