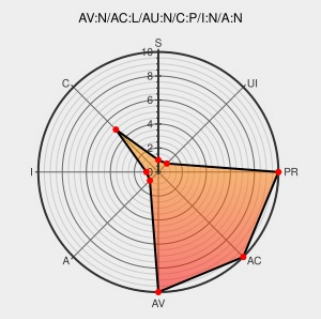
CVE-2011-4138

Published on: 10/19/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:12 PM UTC

CVE-2011-4138

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



Certain versions of Django from Djangoproject contain the following vulnerability:

The verify_exists functionality in the URLField implementation in Django before 1.2.7 and 1.3.x before 1.3.1 originally tests a URL's validity through a HEAD request, but then uses a GET request for the new target URL in the case of a redirect, which might allow remote attackers to trigger arbitrary GET requests with an unintended source IP address via a crafted Location header.

CVE-2011-4138 has been assigned by cve@mitre.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
Django | Weblog | Django 1.2.7 released	Patch, www.djangoproject.com, text/html	CONFIRM www.djangoproject.com/weblog/2011/sep/10/127/
Security Advisory SA46614 - Debian update for python-django - Secunia	web.archive.org, text/html	SECUNIA 46614
oss-security - CVE Request -- Django: v1.3.1, v1.2.7 multiple security flaws	Patch, openwall.com, text/html	MLIST [oss-security] 20110911 CVE Request -- Django: v1.3.1, v1.2.7 multiple security flaws
No Description Provided	hermes.opensuse.org, Inactive Link, Not Archived	SUSE openSUSE-SU-2012:0653

oss-security - Re: CVE Request -- Django: v1.3.1, v1.2.7 multiple security flaws	Patch openwall.com text/html	MLIST [oss-security] 20110913 Re: CVE Request -- Django: v1.3.1, v1.2.7 multiple security flaws
Bug 737366 – CVE-2011-4136 CVE-2011-4137 CVE-2011-4138 CVE-2011-4139 CVE-2011-4140 Django: v1.3.1, v1.2.7 multiple security flaws	Patch bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=737366
September 9 | Weblog | Django	Patch Vendor Advisory www.djangoproject.com text/html	CONFIRM www.djangoproject.com/weblog/2011/sep/09/
Debian -- Security Information -- DSA-2332-1 python-django	www.debian.org Depreciated Link text/html	DEBIAN DSA-2332

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	0.91	All	All	All
Application	Djangoproject	Django	0.95	All	All	All
Application	Djangoproject	Django	0.95.1	All	All	All
Application	Djangoproject	Django	0.96	All	All	All
Application	Djangoproject	Django	1.0	All	All	All
Application	Djangoproject	Django	1.0.1	All	All	All
Application	Djangoproject	Django	1.0.2	All	All	All
Application	Djangoproject	Django	1.1	All	All	All
Application	Djangoproject	Django	1.1.0	All	All	All
Application	Djangoproject	Django	1.1.2	All	All	All
Application	Djangoproject	Django	1.1.3	All	All	All
Application	Djangoproject	Django	1.2	All	All	All
Application	Djangoproject	Django	1.2.1	All	All	All
Application	Djangoproject	Django	1.2.1	2	All	All
Application	Djangoproject	Django	1.2.2	All	All	All
Application	Djangoproject	Django	1.2.3	All	All	All
Application	Djangoproject	Django	1.2.4	All	All	All
Application	Djangoproject	Django	1.2.5	All	All	All

Application	Djangoproject	Django	1.3	All	All	All
Application	Djangoproject	Django	1.3	alpha1	All	All
Application	Djangoproject	Django	1.3	alpha2	All	All
Application	Djangoproject	Django	0.91	All	All	All
Application	Djangoproject	Django	0.95	All	All	All
Application	Djangoproject	Django	0.95.1	All	All	All
Application	Djangoproject	Django	0.96	All	All	All
Application	Djangoproject	Django	1.0	All	All	All
Application	Djangoproject	Django	1.0.1	All	All	All
Application	Djangoproject	Django	1.0.2	All	All	All
Application	Djangoproject	Django	1.1	All	All	All
Application	Djangoproject	Django	1.1.0	All	All	All
Application	Djangoproject	Django	1.1.2	All	All	All
Application	Djangoproject	Django	1.1.3	All	All	All
Application	Djangoproject	Django	1.2	All	All	All
Application	Djangoproject	Django	1.2.1	All	All	All
Application	Djangoproject	Django	1.2.1	2	All	All
Application	Djangoproject	Django	1.2.2	All	All	All
Application	Djangoproject	Django	1.2.3	All	All	All
Application	Djangoproject	Django	1.2.4	All	All	All
Application	Djangoproject	Django	1.2.5	All	All	All
Application	Djangoproject	Django	1.3	All	All	All
Application	Djangoproject	Django	1.3	alpha1	All	All
Application	Djangoproject	Django	1.3	alpha2	All	All
Application	Djangoproject	Django	All	All	All	All

cpe:2.3:a:djangoproject:django:0.91:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:0.95:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:0.95.1:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:0.96:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2.1:2:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2.5:*:*:*:*:*:*:*:

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:alpha2:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:0.91:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:0.95:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:0.95.1:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:0.96:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2.1:2:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:djangoproject:django:1.2.5:*:*:*:*:*:*:*:

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:alpha2:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→