



CVE-2015-8213

Published on: 12/07/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

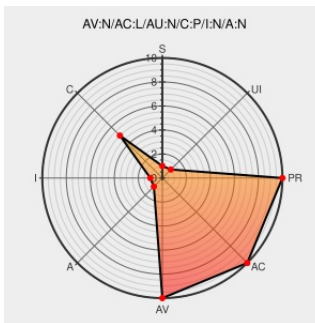
CVE-2015-8213

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Django](#) from [Djangoproject](#) contain the following vulnerability:

The `get_format` function in `utils/formats.py` in Django before 1.7.x before 1.7.11, 1.8.x before 1.8.7, and 1.9.x before 1.9rc2 might allow remote attackers to obtain sensitive application secrets via a settings key in place of a date/time format setting, as demonstrated by `SECRET_KEY`.

CVE-2015-8213 has been assigned by [M](#) 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
Debian -- Security Information -- DSA-3404-1 python-django	www.debian.org Deprecated Link text/html	DEBIAN DSA-3404
USN-2816-1: Django vulnerability Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2816-1
[SECURITY] Fedora 22 Update: python-django-1.8.7-1.fc22	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-323274d412
openSUSE-SU-2015:2199-1: moderate: Security update for python-django	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2199

Security releases issued: 1.9rc2, 1.8.7, 1.7.11 Weblog Django	Patch Vendor Advisory www.djangoproject.com text/html	 CONFIRM www.djangoproject.com/weblog/2015/nov/24/security-releases-issued/
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:0157
Django CVE-2015-8213 Security Bypass Vulnerability	cve.report (archive) text/html	 BID 77750
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:0129
Django Date Template Filter Bug Lets Remote Users Obtain Potentially Sensitive Application Settings Information - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1034237
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:0156
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:0158
Fixed a settings leak possibility in the date template filter. · django/django@316bc3f · GitHub	github.com text/html	 CONFIRM github.com/django/django/commit/316bc3fc9437c5960c24baceb93c73f1939711e4
[SECURITY] Fedora 23 Update: python-django- 1.8.7-1.fc23	lists.fedoraproject.org text/html	 FEDORA FEDORA-2015-a8c8f60fbd
openSUSE-SU- 2015:2202-1: moderate: Security update for python-Django	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2202
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
Application	Djangoproject	Django	1.8.0	All	All	All
Application	Djangoproject	Django	1.8.1	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	1.9.0	rc1	All	All
Application	Djangoproject	Django	1.8.0	All	All	All
Application	Djangoproject	Django	1.8.1	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	1.9.0	rc1	All	All
Application	Djangoproject	Django	All	All	All	All
cpe:2.3:a:djangoproject:django:1.8.0:****:*:*:						
cpe:2.3:a:djangoproject:django:1.8.1:****:*:*:						
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:1.9.0:rc1:****:*:*:						
cpe:2.3:a:djangoproject:django:1.8.0:****:*:*:						
cpe:2.3:a:djangoproject:django:1.8.1:****:*:*:						
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:1.9.0:rc1:****:*:*:						
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](#)