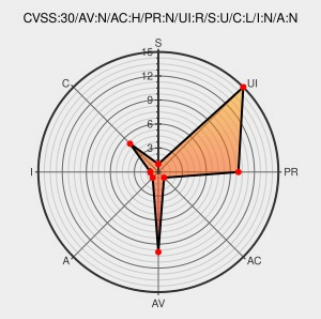
CVE-2016-2513

Published on: 04/08/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:15 PM UTC

CVE-2016-2513

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



Certain versions of Django from Djangoproject contain the following vulnerability:

The password hasher in contrib/auth/hashers.py in Django before 1.8.10 and 1.9.x before 1.9.3 allows remote attackers to enumerate users via a timing attack involving login requests.

CVE-2016-2513 has been assigned by cve@mitre.org to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 3.1 - LOW

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

CVSS2 Score: 2.6 - LOW

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

CVE References

Description	Tags	Link
Oracle Solaris Bulletin - April 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html
Fixed CVE-2016-2513 -- Fixed user enumeration	github.com text/html	CONFIRM github.com/django/django/commit/67b46ba7016da2d259c1ecc7d666d11f5e1cfaab

timing attack during lo… · django/django@67b46ba · GitHub		
Debian -- Security Information -- DSA-3544-1 python-django	www.debian.org Depreciated Link text/html	DEBIAN DSA-3544
USN-2915-2: Django regression | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2915-2
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:0502
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:0505
Django security releases issued: 1.9.3 and 1.8.10 | Weblog | Django	Vendor Advisory www.djangoproject.com text/html	CONFIRM www.djangoproject.com/weblog/2016/mar/01/security-releases/
Django CVE-2016-2513 Security Bypass Vulnerability	cve.report (archive) text/html	BID 83878
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:0506
USN-2915-1: Django vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2915-1
Django Bugs Let Remote Users Conduct Redirect and Cross-Site Scripting Attacks and Determine Valid Usernames - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1035152
USN-2915-3: Django regression | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2915-3
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:0504

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	1.8.9	All	All	All
Application	Djangoproject	Django	1.9	All	All	All
Application	Djangoproject	Django	1.9.1	All	All	All

Application	Djangoproject	Django	1.9.2	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	1.9.2	All	All	All

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:1.9.2:*:*:*:*:*:*:*:

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:1.9.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→