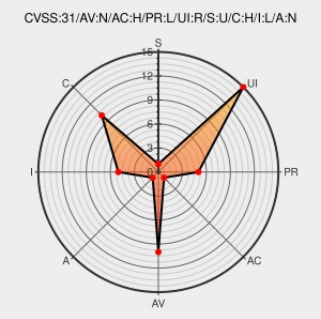
CVE-2020-15105

Published on: 07/10/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15105 - advisory for GHSA-vhr6-pvjm-9qwf

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



Certain versions of Django Two-factor Authentication from Django Two-factor Authentication Project contain the following vulnerability:

Django Two-Factor Authentication before 1.12, stores the user's password in clear text in the user session (base64-encoded). The password is stored in the session when the user submits their username and password, and is removed once they complete authentication by entering a two-factor authentication code. This means that the password is stored in clear text in the session for an arbitrary amount of time, and potentially forever if the user begins the login process by entering their username and password and then leaves before entering their two-factor authentication code. The severity of this issue depends on which type of session storage you have configured: in the worst case, if you're using Django's default database session storage, then users' passwords are stored in clear text in your database. In the best case, if you're using Django's signed cookie session, then users' passwords are only stored in clear text within their browser's cookie store. In the common case of using Django's cache session store, the users' passwords are stored in clear text in whatever cache storage you have configured (typically Memcached or Redis). This has been fixed in 1.12. After upgrading, users should be sure to delete any clear text passwords that have been stored. For example, if you're using the database session backend, you'll likely want to delete any session record from the database and purge that data from any database backups or replicas. In addition, affected organizations who have suffered a database breach while using an affected version should inform their users that their clear text passwords have been compromised. All organizations should encourage users whose passwords were insecurely stored to change these passwords on any sites where they were used. As a workaround, wwitching Django's session storage to use signed cookies instead of the database or cache lessens the impact of this issue, but should not be done without a thorough understanding of the security tradeoffs of using signed cookies rather than a server-side session storage. There is no way to fully mitigate the issue without upgrading.

CVE-2020-15105 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Bouke** - **django-two-factor-auth** version **< 1.12**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.6 - LOW

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

CVE References

Description	Tags	Link
django-two-factor-auth/CHANGELOG.md at master · Bouke/django-two-factor-auth · GitHub	Release Notes, Third Party Advisory, github.com, text/html	MISC github.com/Bouke/django-two-factor-auth/blob/master/CHANGELOG.md#112---2020-07-08
User passwords are stored in clear text in the Django session · Advisory · Bouke/django-two-factor-auth · GitHub	Third Party Advisory, github.com, text/html	CONFIRM github.com/Bouke/django-two-factor-auth/security/advisories/GHSA-vhr6-pvjm-9qwf
Merge pull request from GHSA-vhr6-pvjm-9qwf · Bouke/django-two-factor-auth@454fd98 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/Bouke/django-two-factor-auth/commit/454fd9842fa6e8bb772dbf0943976bc8e3335359

Related QID Numbers

983186 Python (pip) Security Update for django-two-factor-auth (GHSA-vhr6-pvjm-9qwf)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Django Two-factor Authentication Project	Django Two-factor Authentication	All	All	All	All
Application	Django Two-factor Authentication Project	Django Two-factor Authentication	All	All	All	All

cpe:2.3:a:django_two-factor_authentication_project:django_two-factor_authentication:*:*:*:*:*:*:*:*:

cpe:2.3:a:django_two-factor_authentication_project:django_two-factor_authentication:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→