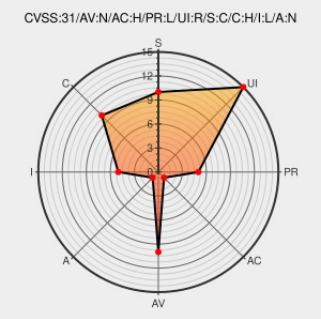
CVE-2020-5224

Published on: 01/24/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:02 PM UTC

CVE-2020-5224 - advisory for GHSA-5fq8-3q2f-4m5g

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



Certain versions of Django-user-sessions from Django-user-sessions Project contain the following vulnerability:

In Django User Sessions (django-user-sessions) before 1.7.1, the views provided allow users to terminate specific sessions. The session key is used to identify sessions, and thus included in the rendered HTML. In itself this is not a problem. However if the website has an XSS vulnerability, the session key could be extracted by the attacker and a session takeover could happen.

CVE-2020-5224 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Jazzband** - **django-user-sessions** version **< 1.7.1**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link

Don't expose session keys in views · jazzband/django-user-sessions@f0c4077 · GitHub	Patch github.com text/html	MISC github.com/jazzband/django-user-sessions/commit/f0c4077e7d1436ba6d721af85cee89222ca5d2d9
Session key exposure through session list · Advisory · jazzband/django-user-sessions · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/Bouke/django-user-sessions/security/advisories/GHSA-5fq8-3q2f-4m5g

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.

Related QID Numbers

983111 Python (pip) Security Update for django-user-sessions (GHSA-5fq8-3q2f-4m5g)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Django-user-sessions Project	Django-user-sessions	All	All	All	All
Application	Django-user-sessions Project	Django-user-sessions	All	All	All	All

cpe:2.3:a:django-user-sessions_project:django-user-sessions:*:*:*:*:*:*:*:*:

cpe:2.3:a:django-user-sessions_project:django-user-sessions:*:*:*:*:*:*:*:*:

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 registred 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