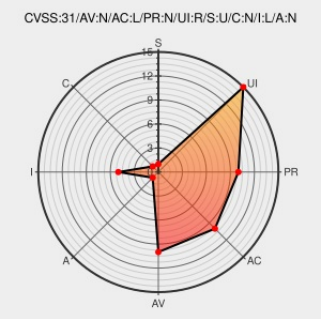
CVE-2023-23608

Published on: Not Yet Published

Last Modified on: 02/06/2023 05:23:00 PM UTC

CVE-2023-23608 - advisory for GHSA-q764-g6fm-555v

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



Certain versions of Spotipy from Spotipy Project contain the following vulnerability:

Spotipy is a light weight Python library for the Spotify Web API. In versions prior to 2.22.1, if a malicious URI is passed to the library, the library can be tricked into performing an operation on a different API endpoint than intended. The code Spotipy uses to parse URIs and URLs allows an attacker to insert arbitrary characters into the path that is used for API requests. Because it is possible to include "..", an attacker can redirect for example a track lookup via spotifyApi.track() to an arbitrary API endpoint like playlists, but this is possible for other endpoints as well. The impact of this vulnerability depends heavily on what operations a client application performs when it handles a URI from a user and how it uses the responses it receives from the API. This issue is patched in version 2.22.1.

CVE-2023-23608 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **spotipy-dev** - **spotipy** version **= < 2.22.1**

CVSS3 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Path traversal vulnerability that may lead to type confusion in URI handling code · Advisory · spotipy-dev/spotipy · GitHub	github.com text/html	MISC github.com/spotipy-dev/spotipy/security/advisories/GHSA-q764-g6fm-555v

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

691050 Free Berkeley Software Distribution (FreeBSD) Security Update for spotipy (c3fb48cc-a2ff-11ed-8fbc-6cf0490a8c18)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Spotipy Project	Spotipy	All	All	All	All

cpe:2.3:a:spotipy_project:spotipy:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→