CVE-2023-22903

LibrePhotos - CVSS 3.x 9.8 CRITICAL

In 2022-Q2, Librephotos, an open-source self hosted photo cloud solution, introduced an Remote Information Disclosure Vulnerability. This allowed an attacker to obtain a list of users': Full name, Email address, Photo count, Nextcloud Configuration and various other data points.

Software versions between 2022w19 to 2022w50, released in December 2022, are vulnerable to this attack. It is advised all administrators upgrade urgently.

Vulnerability Categorisation

Severity: CRITICAL
Vendor: LibrePhotos (open-source)
Vulnerability Type: Incorrect Access Control
Attack Type: Remote
Impact: Information Disclosure
Attack Vectors: REST API
Affected Component: api/user.py
Sophistication: Low

Zero-Day Exploitation

Exploited In Wild: Unknown
Notes: Due to the very low sophistication it is very possible this exploit has been used in the wild.

Vulnerability Attack Vector

To exploit this vulnerability an attacker must send a unauthenticated HTTP request to:

```
GET /api/users/?format=json
```

Affected Component

The vulnerability was caused due to incorrect access control. The API route, programmed at: api/user.py, did not check for authorisation, allowing anyone to query the sensitive API's data.

This vulnerability has been patched in 2023w08. The vendor has re-factored the API to return non-sensitive information. Additionally, the API only features users which explicitly opt-in to publicly displaying membership.