



CVE-2022-39230

Published on: Not Yet Published

Last Modified on: 09/26/2022 05:20:00 PM UTC

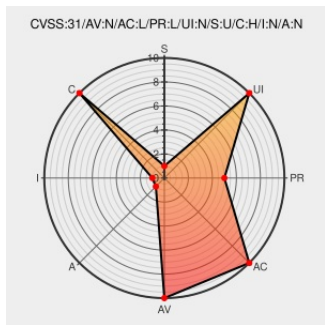
CVE-2022-39230 - advisory for GHSA-vv7x-7w4m-q72f

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Fhir-works-on-aws-authz-smart](#) from [Amazon](#) contain the following vulnerability:

fhir-works-on-aws-authz-smart is an implementation of the authorization interface from the FHIR Works interface. Versions 3.1.1 and 3.1.2 are subject to Exposure of Sensitive Information to an Unauthorized Actor. This issue allows a client of the API to retrieve more information than the client's OAuth scope permits when making

“search-type” requests. This issue would not allow a client to retrieve information about individuals other than those the client was already authorized to access. Users of fhir-works-on-aws-authz-smart 3.1.1 or 3.1.2 should upgrade to version 3.1.3 or higher immediately. Versions 3.1.0 and below are unaffected. There is no workaround for this issue.

CVE-2022-39230 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **awslabs - fhir-works-on-aws-authz-smart** version > 3.1.0, < 3.1.3

CVSS3 Score: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
Security issue in fhir-works-on-aws-authz-smart · Advisory · awslabs/fhir-works-on-aws-authz-smart · GitHub	github.com text/html	CONFIRM github.com/awslabs/fhir-works-on-aws-authz-smart/security/advisories/GHSA-vv7x-7w4m-q72f

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.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

fhir-works-on-aws-authz-smart is an implementation of the authorization interface from the FHIR Works interface. Vers...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Amazon	Fhir-works-on-aws-authz-smart	All	All	All	All
cpe:2.3:a:amazon:fhir-works-on-aws-authz-smart:*:*:*:*:*.*.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-39230 : fhir-works-on-aws-authz-smart is an implementation of the authorization interface from the FHIR Wo... twitter.com/i/web/status/1...	2022-09-23 07:16:04
 /r/netcve	CVE-2022-39230	2022-09-23 08:38:12

[← 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 registered 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](#)