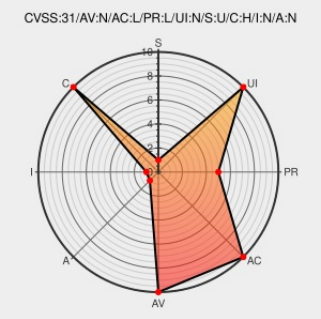
CVE-2023-32060

Published on: Not Yet Published

Last Modified on: 05/16/2023 05:04:00 PM UTC

CVE-2023-32060 - advisory for GHSA-7pwm-6rh2-2388

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



Certain versions of Dhis 2 from Dhis2 contain the following vulnerability:

DHIS2 Core contains the service layer and Web API for DHIS2, an information system for data capture. Starting in the 2.35 branch and prior to versions 2.36.13, 2.37.8, 2.38.2, and 2.39.0, when the Category Option Combination Sharing settings are configured to control access to specific tracker program events or program stages, the `/trackedEntityInstances` and `/events` API endpoints may include all events regardless of the sharing settings applied to the category option combinations. When this specific configuration is present, users may have access to events which they should not be able to see based on the sharing settings of the category options. The events will not appear in the user interface for web-based Tracker Capture or Capture applications, but if the Android Capture App is used they will be displayed to the user. Versions 2.36.13, 2.37.8, 2.38.2, and 2.39.0 contain a fix for this issue. No workaround is known.

CVE-2023-32060 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **dhis2** - **dhis2-core** version **= >= 2.35, < 2.36.13**

Affected Vendor/Software: **dhis2** - **dhis2-core** version **= >= 2.37, < 2.37.8**

Affected Vendor/Software: **dhis2** - **dhis2-core** version **= >= 2.38, < 2.38.2**

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
Improper Access Control with Category Option Combination sharing in /api/trackedEntityInstance and /api/events · Advisory · dhis2/dhis2-core · GitHub	github.com text/html	MISC github.com/dhis2/dhis2-core/security/advisories/GHSA-7pwm-6rh2-2388

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dhis2	Dhis 2	All	All	All	All

cpe:2.3:a:dhis2:dhis_2:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-32060 : DHIS2 Core contains the service layer and Web API for DHIS2, an information system for data captur… twitter.com/i/web/status/1…	2023-05-09 15:04:40

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report