



# CVE-2023-31139

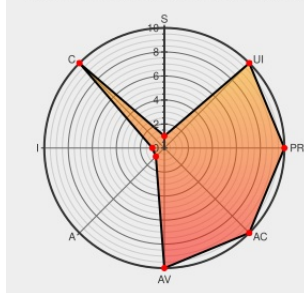
Published on: Not Yet Published

Last Modified on: 05/16/2023 04:50:00 PM UTC

## CVE-2023-31139 - advisory for GHSA-44g3-9mp4-prv3

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N



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 2.37 branch and prior to versions 2.37.9.1, 2.38.3.1, and 2.39.1.2, Personal Access Tokens (PATs) generate unrestricted session cookies. This may lead to a bypass of other access restrictions (for example, based on allowed IP addresses or HTTP methods). DHIS2 implementers should upgrade to a supported version of DHIS2: 2.37.9.1, 2.38.3.1, or 2.39.1.2. Implementers can work around this issue by adding extra access control validations on a reverse proxy.

CVE-2023-31139 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [dhis2](#) - **dhis2-core** version = **>= 2.37, < 2.37.9.1**

Affected Vendor/Software: [dhis2](#) - **dhis2-core** version = **>= 2.38, < 2.38.3.1**

Affected Vendor/Software: [dhis2](#) - **dhis2-core** version = **>= 2.39, < 2.39.1.2**

CVSS3 Score: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |

## CVE References

| Description                                                                      | Tags                                                    | Link                                                                                     |
|----------------------------------------------------------------------------------|---------------------------------------------------------|------------------------------------------------------------------------------------------|
| Unrestricted session cookies with PATs · Advisory · dhis2/dhis2-core · GitHub    | <a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">MISC github.com/dhis2/dhis2-core/security/advisories/GHSA-44g3-9mp4-prv3</a> |
| dhis2-releases/ReleaseNote-2.39.1.2.md at master · dhis2/dhis2-releases · GitHub | <a href="#">github.com</a>                              | <a href="#">MISC github.com/dhis2/dhis2-releases/ReleaseNote-2.39.1.2.md</a>             |

|                                                                                                  |                                                         |                                                                                                        |
|--------------------------------------------------------------------------------------------------|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| <a href="#">dhis2-releases/ReleaseNote-2.39.1.2.md at master · dhis2/dhis2-releases · GitHub</a> | <a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">MISC github.com/dhis2/dhis2-releases/blob/master/releases/2.39/ReleaseNote-2.39.1.2.md</a> |
| <a href="#">dhis2-releases/ReleaseNote-2.37.9.1.md at master · dhis2/dhis2-releases · GitHub</a> | <a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">MISC github.com/dhis2/dhis2-releases/blob/master/releases/2.37/ReleaseNote-2.37.9.1.md</a> |
| <a href="#">dhis2-releases/ReleaseNote-2.38.3.1.md at master · dhis2/dhis2-releases · GitHub</a> | <a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">MISC github.com/dhis2/dhis2-releases/blob/master/releases/2.38/ReleaseNote-2.38.3.1.md</a> |

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](mailto: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-2023-31139 : DHIS2 Core contains the service layer and Web API for DHIS2, an information system for data captur... <a href="#">twitter.com/i/web/status/1...</a> | 2023-05-09 15:03:45 |

[← Previous ID](#)

[Next ID →](#)