

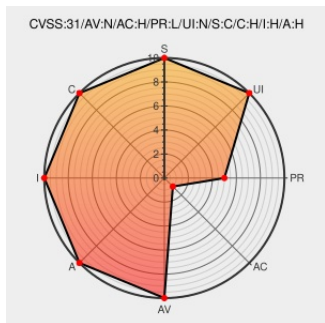


CVE-2021-32704

Published on: 06/24/2021 12:00:00 AM UTC

Last Modified on: 07/08/2021 02:09:00 PM UTC

CVE-2021-32704 - advisory for GHSA-fj38-585h-hxgj

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

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

DHIS 2 is an information system for data capture, management, validation, analytics and visualization. A SQL injection security vulnerability has been found in specific versions of DHIS2. This vulnerability affects the `/api/trackedEntityInstances` API endpoint in DHIS2 versions 2.34.4, 2.35.2, 2.35.3, 2.35.4, and 2.36.0. Earlier

versions, such as 2.34.3 and 2.35.1 and all versions 2.33 and older are unaffected. The system is vulnerable to attack only from users that are logged in to DHIS2, and there is no known way of exploiting the vulnerability without first being logged in as a DHIS2 user. A successful exploit of this vulnerability could allow the malicious user to read, edit and delete data in the DHIS2 instance. There are no known exploits of the security vulnerabilities addressed by these patch releases. However, we strongly recommend that all DHIS2 implementations using versions 2.34, 2.35 and 2.36 install these patches as soon as possible. There is no straightforward known workaround for DHIS2 instances using the Tracker functionality other than upgrading the affected DHIS2 server to one of the patches in which this vulnerability has been fixed. For implementations which do NOT use Tracker functionality, it may be possible to block all network access to POST to the `/api/trackedEntityInstance` endpoint as a temporary workaround while waiting to upgrade.

CVE-2021-32704 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **dhis2** - **dhis2-core** version `>= 2.34.4, < 2.34.5`

Affected Vendor/Software: **dhis2** - **dhis2-core** version `>= 2.35.2, < 2.35.5`

Affected Vendor/Software: **dhis2** - **dhis2-core** version `>= 2.36.0, < 2.36.1`

CVSS3 Score: **8.8 - HIGH**

Attack
Vector

NETWORK

Attack
Complexity

LOW

Privileges
Required

LOW

User
Interaction

NONE

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH
CVSS2 Score: 6.5 - MEDIUM			
Access Vector	Access Complexity	Authentication	
NETWORK	LOW	SINGLE	
Confidentiality Impact	Integrity Impact	Availability Impact	
PARTIAL	PARTIAL	PARTIAL	

CVE References

Description	Tags	Link
SQL Injection in DHIS2 Tracker API · Advisory · dhis2/dhis2-core · GitHub	github.com text/html	CONFIRM github.com/dhis2/dhis2-core/security/advisories/GHSA-fj38-585h-hxgj

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-2021-32704 : DHIS 2 is an information system for data capture, management, validation, analytics and visualizat... twitter.com/i/web/status/1...	2021-06-24 16:12:35
 /r/netcve	CVE-2021-32704	2021-06-24 16:41:34

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](#)