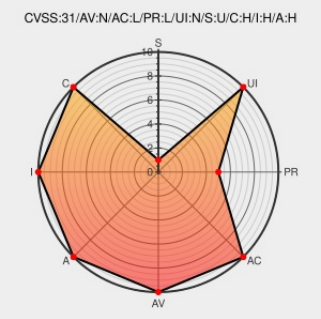
CVE-2021-39179

Published on: 10/29/2021 12:00:00 AM UTC

Last Modified on: 11/03/2021 12:55:00 AM UTC

CVE-2021-39179 - advisory for GHSA-cmpc-frjv-rrmw

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 vulnerability in the Tracker component in DHIS2 Server allows authenticated remote attackers to execute arbitrary SQL commands via unspecified vectors. This vulnerability affects the `/api/trackedEntityInstances` and `/api/trackedEntityInstances/query` API endpoints in all DHIS2 versions 2.34, 2.35, and 2.36. It also affects versions 2.32 and 2.33 which have reached _end of support_ - exceptional security updates have been added to the latest *end of support* builds for these versions. Versions 2.31 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. The vulnerability is not exposed to a non-malicious user - the vulnerability requires a conscious attack to be exploited. 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. Security patches are available in DHIS2 versions 2.32-EOS, 2.33-EOS, 2.34.7, 2.35.7, and 2.36.4. 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/trackedEntityInstances`, and `/api/trackedEntityInstances/query` endpoints as a temporary workaround while waiting to upgrade.

CVE-2021-39179 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **dhis2** - **dhis2-core** version **= 2.32**

Affected Vendor/Software: **dhis2** - **dhis2-core** version **= 2.33**

Affected Vendor/Software: **dhis2** - **dhis2-core** version **>= 2.34.0, < 2.34.7**

Affected Vendor/Software: **dhis2** - **dhis2-core** version **>= 2.34.0, < 2.35.7**

Affected Vendor/Software: **dhis2** - **dhis2-core** version **>= 2.36.0, < 2.36.4**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	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
build: correct patch PRs (#8771) · dhis2/dhis2-core@16674ac · GitHub	github.com text/html	MISC github.com/dhis2/dhis2-core/commit/16674ac75127b0e83691c6b1c9ce745e67ab58b6
SQL Injection in DHIS2 Tracker API (assignedUsers and escapeSql) · Advisory · dhis2/dhis2-core · GitHub	github.com text/html	CONFIRM github.com/dhis2/dhis2-core/security/advisories/GHSA-cmpc-frjv-rrmw
build: correct patch PRs by Philip-Larsen-Donnelly · Pull Request #8771 · dhis2/dhis2-core · GitHub	github.com text/html	MISC github.com/dhis2/dhis2-core/pull/8771

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
Application	Dhis2	Dhis 2	All	All	All	All
Application	Dhis2	Dhis 2	All	All	All	All

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

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-39179 : DHIS 2 is an information system for data capture, management, validation, analytics and visualizat… twitter.com/i/web/status/1…	2021-10-29 13:28:12
@0_exploit	CVE-2021-39179 dlvr.it/SBXnRr	2021-10-29 17:37:05
@threatmeter	CVE-2021-39179 DHIS 2 is an information system for data capture, management, validation, analytics and visualizatio… twitter.com/i/web/status/1…	2021-10-30 07:09:58

← Previous ID

Next ID→