

SQL Injection in DHIS2 Tracker API (assignedUsers and escapeSql)

Moderate
Philip-Larsen-Donnelly published GHSA-cmpc-frjv-rrmw on Oct 29, 2021

Package	
dhis2-core (none)	
Affected versions	Patched versions
2.32, 2.33, 2.35, 2.36	2.32-EOS, 2.33-EOS, 2.35.7, 2.36.4

Description

Description

Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in the Tracker component in DHIS2 Server allows authenticated remote attackers to execute arbitrary SQL commands via unspecified vectors.

Impact

A serious SQL injection security vulnerability has been found in specific versions of DHIS2. This vulnerability affects the `/api/trackedEntityInstances` and `/api/trackedEntityInstances/query` API endpoints in all DHIS2 versions 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.

Version 2.34 as well as 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. However, we strongly recommend that all DHIS2 implementations using versions 2.32, 2.33, 2.35 and 2.36 install these patches as soon as possible.

Patches

Security patches are now available for the following DHIS2 versions:

v2.32 -- Update to the latest v2.32-EOS
v2.33 -- Update to the latest v2.33-EOS
v2.35 -- Update to v2.35.7
v2.36 -- Update to v2.36.4

These patches address a critical security vulnerability. If your DHIS2 system is using one of the versions listed above, you should download and install the appropriate patch version immediately. All latest patch versions are available for download at [dhis2.org/downloads](#).

Workarounds

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 or events functionality, it may be possible to block all network access to the `/api/trackedEntityInstances` and `/api/trackedEntityInstances/query` endpoints as a temporary workaround while waiting to upgrade.

References

You can read more about the process for identifying, reviewing, and addressing potential security vulnerabilities on our website: <https://dhis2.org/security>

For more information

If you have any questions or comments about this advisory:

Email us at security@dhis2.org

Severity

Moderate





CVE ID

CVE-2021-39179

Weaknesses

CWE-89

Credits

-  ameenhere
-  gnespolino
-  Bekkalizer
-  Philip-Larsen-Donnelly