

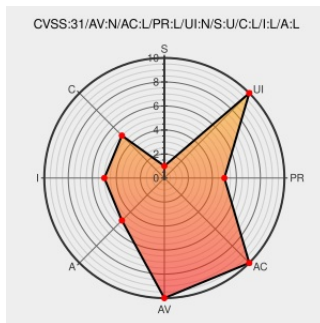


CVE-2020-11010

Published on: 04/20/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:24 PM UTC

CVE-2020-11010 - advisory for GHSA-9j2c-x8qm-qmjq

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

Certain versions of [TortoiseOrm](#) from [TortoiseOrm Project](#) contain the following vulnerability:

In Tortoise ORM before versions 0.15.23 and 0.16.6, various forms of SQL injection have been found for MySQL and when filtering or doing mass-updates on char/text fields. SQLite & PostgreSQL are only affected when filtering with contains, starts_with, or ends_with filters (and their case-insensitive counterparts).

CVE-2020-11010 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [tortoise](#) - [tortoise-orm](#) version < 0.15.23

Affected Vendor/Software: [tortoise](#) - [tortoise-orm](#) version >= 0.16.0, < 0.16.6

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	Taas	Link
-------------	------	------

Fixed various SQL generation issues · tortoise/tortoise-orm@91c3640 · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC

github.com/tortoise/tortoise-orm/commit/91c364053e0ddf77edc5442914c6f049512678b3

Various SQL injection attacks have been mitigated. · Advisory · tortoise/tortoise-orm · GitHub

Third Party Advisory

github.com

text/html

CONFIRM

github.com/tortoise/tortoise-orm/security/advisories/GHSA-9j2c-x8qm-qmjq

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.

Related QID Numbers

983127 Python (pip) Security Update for tortoise-orm (GHSA-9j2c-x8qm-qmjq)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tortoise Orm Project	Tortoise Orm	All	All	All	All
Application	Tortoise Orm Project	Tortoise Orm	All	All	All	All

cpe:2.3:a:tortoise_orm_project:tortoise_orm:*:*:*:*:*:

cpe:2.3:a:tortoise_orm_project:tortoise_orm:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →