TaffyDB can allow access to any data items in the DB

Opened 2 months ago on taffydb (npm) · package-lock.json

Severity
High 7.5 / 10

TaffyDB allows attackers to forge adding additional properties into user-input processed by taffy which can allow access to any data items in the DB. Taffy sets an internal index for each data item in its DB. However, it is found that the internal index can be forged by adding additional properties into user-input. If index is found in the query, TaffyDB will ignore other query conditions and directly return the indexed data item. Moreover, the internal index is in an easily-guessable format (e.g., T000002R000001). As such, attackers can use this vulnerability to access any data items in the DB. **Note:** taffy and its successor package taffydb are not maintained.

Tags
Development dependency

Weaknesses
- CWE-20
- CWE-668

CVE ID
CVE-2019-10790

GHSA ID
GHSA-mxhp-79qh-mcx6

See advisory in GitHub Advisory Database