

Dependabot alerts / #10

TaffyDB can allow access to any data items in the DB #10

Dismiss alert ▾

Open

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

Package	Affected versions	Patched version
taffydb (npm)	<= 2.7.3	None

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.

Severity

High 7.5 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	None
Availability	None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

dependabot bot opened this 2 months ago

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

 [See all of your affected repositories](#)

See something to contribute?
[Suggest improvements for this advisory on the GitHub Advisory Database.](#)