



CVE-2020-4035

Published on: 06/03/2020 12:00:00 AM UTC

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

CVE-2020-4035 - advisory for GHSA-38f9-m297-6q9g

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

CVSS:31/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H



Certain versions of [Watermelondb](#) from [Nozbe](#) contain the following vulnerability:

In WatermelonDB (NPM package "@nozbe/watermelondb") before versions 0.15.1 and 0.16.2, a maliciously crafted record ID can exploit a SQL Injection vulnerability in iOS adapter implementation and cause the app to delete all or selected records from the database, generally causing the app to become unusable. This may happen in apps that

don't validate IDs (valid IDs are `/^[a-zA-Z0-9_-.]+$/`) and use Watermelon Sync or low-level ``database.adapter.destroyDeletedRecords`` method. The integrity risk is low due to the fact that maliciously deleted records won't synchronize, so logout-login will restore all data, although some local changes may be lost if the malicious deletion causes the sync process to fail to proceed to push stage. No way to breach confidentiality with this vulnerability is known. Full exploitation of SQL Injection is mitigated, because it's not possible to nest an insert/update query inside a delete query in SQLite, and it's not possible to pass a semicolon-separated second query. There's also no known practicable way to breach confidentiality by selectively deleting records, because those records will not be synchronized. It's theoretically possible that selective record deletion could cause an app to behave insecurely if lack of a record is used to make security decisions by the app. This is patched in versions 0.15.1, 0.16.2, and 0.16.1-fix

CVE-2020-4035 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Nozbe - WatermelonDB** version < 0.15.1

Affected Vendor/Software: **Nozbe - WatermelonDB** version >= 0.16.0, < 0.16.2

CVSS3 Score: **5.9 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	NONE
Scope	Confidentiality	Integrity	Availability

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	LOW	HIGH
CVSS2 Score: 5.5 - MEDIUM			
Access Vector	Access Complexity	Authentication	
NETWORK	LOW	SINGLE	
Confidentiality Impact	Integrity Impact	Availability Impact	
NONE	PARTIAL	PARTIAL	

CVE References

Description	Tags	Link
Fix destroyDeletedRecords vulnerability · Nozbe/WatermelonDB@924c7ae · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/Nozbe/WatermelonDB/commit/924c7ae2a8d7d6459656751e5b9b1bf91a
DoS or local data modification via malicious record IDs · Advisory · Nozbe/WatermelonDB · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/Nozbe/WatermelonDB/security/advisories/GHSA-38f9-m2

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

983399 Nodejs (npm) Security Update for @nozbe/watermelondb (GHSA-38f9-m297-6q9g)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nozbe	Watermelondb	All	All	All	All
Application	Nozbe	Watermelondb	0.16.0	All	All	All
Application	Nozbe	Watermelondb	0.16.1	All	All	All
Application	Nozbe	Watermelondb	All	All	All	All
Application	Nozbe	Watermelondb	0.16.0	All	All	All
Application	Nozbe	Watermelondb	0.16.1	All	All	All
cpe:2.3:a:nobbe:watermelondb:*.*.*.*.*.*.*.*.						
cpe:2.3:a:nobbe:watermelondb:0.16.0:*.*.*.*.*.*.*.*.						
cpe:2.3:a:nobbe:watermelondb:0.16.1:*.*.*.*.*.*.*.*.						

cpe:2.3:a:nozbe:watermelondb:*:*:*:*:*:*:

cpe:2.3:a:nozbe:watermelondb:0.16.0:*:*:*:*:*:

cpe:2.3:a:nozbe:watermelondb:0.16.1:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)