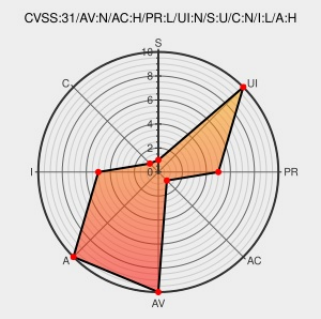
CVE-2020-4035

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



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/924c7ae2a8d7d6459656751e5b9b1bf91
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

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:nozbe:watermelondb:*:*:*:*:*:*:*:*:

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

cpe:2.3:a:nozbe: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→