Server hangs when using specific clumplet on batch creation

Moderate **dyemanov** published **GHSA-7cq5-994r-jhrf** 3 days ago

Package

No package listed

Affected versions	Patched versions
Versions >= 4 (v3 was not tested but the code is the same)	6.0, 5.0.4, 4.0.7, 3.0.14

Description

Summary

Incorrect parsing of clumplet allows authenticated user to DoS the server.

Details

The main bug is in the `ClumpletReader::getClumpletSize()` function, It is possible to overflow `totalLength` when parsing `Wide` type, which can lead to an infinite loop. I have found that this can be exploited in batch clumplet (there may be other ways in which it can be abused that I have not yet figured out).
The following is an example of a stack trace when this vulnerability is exploited:

▶ Stacktrace

Therefore, if an authenticated user has the INSERT privilege for a given table, they can create an infinite number of requests that will cause a DoS attack on the server.

PoC

I created a database with one table and granted the user INSERT privileges for that table. Then I attached it, started a transaction and created a batch with specific bpb (Batch Parameter Block) (this bpb can be found inside the Program below).
I wrote a simple C++ program to reproduce this:

▶ Program

Impact

Essentially, every server is affected.

Patch with fix

I have write a possible fix for this issue:

▶ Patch diff

Severity

Moderate

CVE ID

CVE-2026-28214

Weaknesses

No CWEs