README

CVE-2026-29628 tinyobjloader experimental parser buffer overflow

Summary

Stack-based buffer overflow overflow in https://github.com/tinyobjloader/tinyobjloader, it only affects the experimental version, which can lead to unexpected results.

Affected versions

`tinyobjloader` is affected in all versions up to commit `d56555b`.

A fix was proposed in:

- `386b73bb8c1a855236beb73b11f45f7feac4e03a`
  https://github.com/kiyochii/tinyobjloader/tree/386b73bb8c1a855236beb73b11f45f7feac4e03a

Repository:

- https://github.com/tinyobjloader/tinyobjloader

Proof of Concept

The issue is reproducible under AddressSanitizer as a stack-buffer-overflow in `tinyobj_opt::LoadMtl`, where an oversized `newmtl token` is written into the fixed-size local buffer `namebuf`.

Compile Instructions

Build the proof of concept with AddressSanitizer and UndefinedBehaviorSanitizer enabled:

```
clang++ -std=c++17 -O1 -g -fsanitize=address,undefined -fno-omit-frame-pointer \
  -I./tinyobjloader \
```

Releases

No releases published

Packages

No packages published

Contributors

No contributors

Languages

- **C++** 100.0%