October 14, 2022

GHSL-2022-066: Stack Buffer Overflow in iowow - CVE-2022-23462

GitHub Security Lab

Coordinated Disclosure Timeline

- 2022-08-24: Reported to Anton Adamansky, the lead maintainer
- 2022-08-25: Issue has been addressed with commit
- 2022-08-27: Maintainer has delayed response to requests for security advisory.
- 2022-09-06: Assigned CVE-2022-23462

Summary

There is a stack buffer overflow present in iowow that allows for Denial of Service (DOS) when it parses scientific notation numbers present in JSON.

Product

iowow

Tested Version

Latest

Details

Issue: stack buffer overflow in `iwjson.c` (`GHSL-2022-066`)

```
void iwjson_ftoa(long double val, char buf[static IWNUMBUF_SIZE], size_t *out_len) {
            int len = snprintf(buf, 64, "%.8Lf", val);
```

`buf` has size `IWNUMBUF_SIZE` (32) but the format string assumes a size of 64 resulting in a stack buffer overflow. This allows for DOS due to a stack canary overwrite. Without a stack canary, instruction pointer can be overwritten with numerical values 0x30 to 0x39.

Impact

This issue may lead to Denial of Service (DOS).

CVE

- CVE-2022-23462

Credit

This issue was discovered and reported by GHSL team member @Kwstubbs (Kevin Stubbings).

Contact

You can contact the GHSL team at `securitylab@github.com`, please include a reference to `GHSL-2022-066` in any communication regarding this issue.

- Careers
- Press
- Shop

- 
- 
- 
- 
-