Integer Overflow in Chunked Transfer-Encoding

Moderate **seanmonstar** published **GHSA-5h46-h7hh-c6x9** on Jul 7, 2021

Package	
hyper (crates.io)	
Affected versions	Patched versions
< 0.14.10	0.14.10

Description

Summary

hyper's HTTP server and client code had a flaw that could trigger an integer overflow when decoding chunk sizes that are too big. This allows possible data loss, or if combined with an upstream HTTP proxy that allows chunk sizes larger than hyper does, can result in "request smuggling" or "desync attacks".

Vulnerability

Example:

```
GET / HTTP/1.1
Host: example.com
Transfer-Encoding: chunked

f0000000000000003
abc
0
```

hyper only reads the rightmost 64-bit integer as the chunk size. So it reads `f0000000000000003` as `3`. A loss of data can occur since hyper would then read only 3 bytes of the body. Additionally, an HTTP request smuggling vulnerability would occur if using a proxy which instead has prefix truncation in the chunk size, or that understands larger than 64-bit chunk sizes.

Read more about desync attacks: https://portswigger.net/research/http-desync-attacks-request-smuggling-reborn

Impact

To determine if vulnerable to *data loss*, these things must be true:

- **Using HTTP/1.1.** Since HTTP/2 does not use chunked encoding, it is not vulnerable.
- **Using hyper as a server or client.** The body would be improperly truncated in either case.
- **Users send requests or responses with chunk sizes greater than 18 exabytes.**

To determine if vulnerable to *desync attacks*, these things must be true:

- **Using an upstream proxy that allows chunks sizes larger than 64-bit.** If the proxy rejects chunk sizes that are too large, that request won't be forwarded to hyper.

Patches

We have released the following patch versions:

- v0.14.10 (to be released when this advisory is published)

Workarounds

Besides upgrading hyper, you can take the following options:

- Reject requests manually that contain a `Transfer-Encoding` header.
- Ensure any upstream proxy rejects `Transfer-Encoding` chunk sizes greater than what fits in 64-bit unsigned integers.

Credits

This issue was initially reported by Mattias Grenfeldt and Asta Olofsson.

Severity

Moderate

CVE ID

CVE-2021-32714

Weaknesses

CWE-190

Credits

mattiasgrenfeldt

asta12