Reallocation bug can trigger heap memory corruption

Moderate **brianmario** published **GHSA-jj47-x69x-mxrm** on Apr 5

Package

yajl-ruby (RubyGems)

Affected versions	Patched versions
<= 1.4.2	1.4.3

Description

NOTE: A previous patch, 1.4.2, fixed the heap memory issue, but could still lead to a DoS infinite loop. Please update to version 1.4.3

The 1.x branch and the 2.x branch of yajl contain an integer overflow which leads to subsequent heap memory corruption when dealing with large (~2GB) inputs.

Details

The reallocation logic at yajl_buf.c#L64 may result in the `need` 32bit integer wrapping to 0 when `need` approaches a value of 0x80000000 (i.e. ~2GB of data), which results in a reallocation of buf->alloc into a small heap chunk.

These integers are declared as `size_t` in the 2.x branch of `yajl`, which practically prevents the issue from triggering on 64bit platforms, however this does not preclude this issue triggering on 32bit builds on which `size_t` is a 32bit integer.

Subsequent population of this under-allocated heap chunk is based on the original buffer size, leading to heap memory corruption.

Impact

We rate this as a moderate severity vulnerability which mostly impacts process availability as we believe exploitation for arbitrary code execution to be unlikely.

Patches

Patched in yajl-ruby 1.4.3

Workarounds

Avoid passing large inputs to YAJL

References

yajl-ruby/ext/yajl/yajl_buf.c
Line 64 in 7168bd7

```
64      while (want >= (need - buf->used)) need <<= 1;
```

For more information

If you have any questions or comments about this advisory:

- Open an issue in yajl-ruby

Severity

Moderate 5.9 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID

CVE-2022-24795

Weaknesses

CWE-122 CWE-190

Credits

jhawthorn