ADA LOGICS

Lima Fuzzing Audit 2024

Lima Fuzzing Audit Report

In collaboration with the Cloud Native Computing Foundation and the Lima Maintainers

Adam Korczynski, David Korczynski

23rd September 2024

Contents

CNCF security and fuzzing audits

This report details a fuzzing audit commissioned by the CNCF and the engagement is part of the broader efforts carried out by CNCF in securing the software in the CNCF landscape. Demonstrating and ensuring the security of these software packages is vital for the CNCF ecosystem and the CNCF continues to use state of the art techniques to secure its projects as well as carrying out manual audits. Over the last handful of years, CNCF has been investing in security audits, fuzzing and software supply chain security that has helped proactively discover and fix hundreds of issues.

Fuzzing is a proven technique for finding security and reliability issues in software and the efforts so far have enabled fuzzing integration into more than twenty CNCF projects through a series of dedicated fuzzing audits. In total, more than 350 bugs have been found through fuzzing of CNCF projects. The fuzzing efforts of CNCF have focused on enabling continuous fuzzing of projects to ensure continued security analysis, which is done by way of the open source fuzzing project OSS-Fuzz.

CNCF continues work in this space and will further increase investment to improve security across its projects and community. The focus for future work is integrating fuzzing into more projects, enabling sustainable fuzzer maintenance, increasing maintainer involvement and enabling fuzzing to find more vulnerabilities in memory safe languages. Maintainers who are interested in getting fuzzing integrated into their projects or have questions about fuzzing are encouraged to visit the dedicated cncf-fuzzing repository https://github.com/cncf/cncf-fuzzing where questions and queries are welcome.

Executive summary

In this engagement, Ada Logics worked on setting up a fuzzing suite for Lima. At the time that this engagement started, Lima did not have or do any fuzz testing, and the goal of this fuzzing audit was to build the infrastructure that would support an integration into OSS-Fuzz and then improve the fuzzing efforts in a continuous manner. The integration into OSS-Fuzz allows Limas fuzzers to run continuously during the audit as well as after our work during this audit has concluded. This is important for Limas, since Lima will continue to be fuzz tested as the project changes over time.

We carried out this work in collaboration with the Lima maintainers which allowed us to efficiently get the fuzz tests checked into Limas source tree. This is arguably the best way to store a projects fuzzers in general, as the maintainers have the highest degree of control of the fuzzing suite.

We wrote a total of 8 fuzzers with a focus on APIs with a large call graph as well as with a high level of complexity.

Strategic recommendations

There are a few key takeaways from this engagement. The first is that fuzzing finds issues in Lima and as such provides value. We expect that the fuzzers will continue to find issues in 3rd-party parsers for a while and then stagnate in terms of quantity. Therefore, we highly recommend that the Lima community maintains the fuzzing suite at minimum to allow the fuzzers to be functional and run on OSS-Fuzz.

Lima developers do not need to run the fuzzers locally; OSS-Fuzz is far more efficient than any contributors local machine. That being said, Lima can consider adding OSS-Fuzz's CI action (https://google.github.io/oss-fuzz/getting-started/continuous-integration/) to fuzz code before it is merged into Limas source repository.

The biggest take-away from the issues found from this engagement is that Limas 3rd-party YAML parsers are highly prone to bugs. From our evaluation, the vast majority of crashes found by the fuzzers during the engagement require upstream fixes in 3rd-party dependencies. Some of these dependencies are slow to respond to bug fixes and do not have the proper channels to report security issues. An example of such depdency is `https://github.com/goccy/go-yaml` which seems unable to respond to pull requests and security disclosures in a manner that could be acceptable to Lima. We recommend that Lima considers its position to bugs from its depencies. Once the current crashes are fixed, the fuzzers will be able to progress and reach further into Limas dependencies, and the fuzzers are likely to find more issues in these libraries.

Lima fuzzing

In this section we present details on the Lima fuzzing set up. We first present a high-level view of the overall fuzzing architecture and how it supports running the fuzzers continuously. We then enumerate the fuzzers we wrote during the audit, and finally we go into detail with the crashes that the fuzzers found.

Architecture

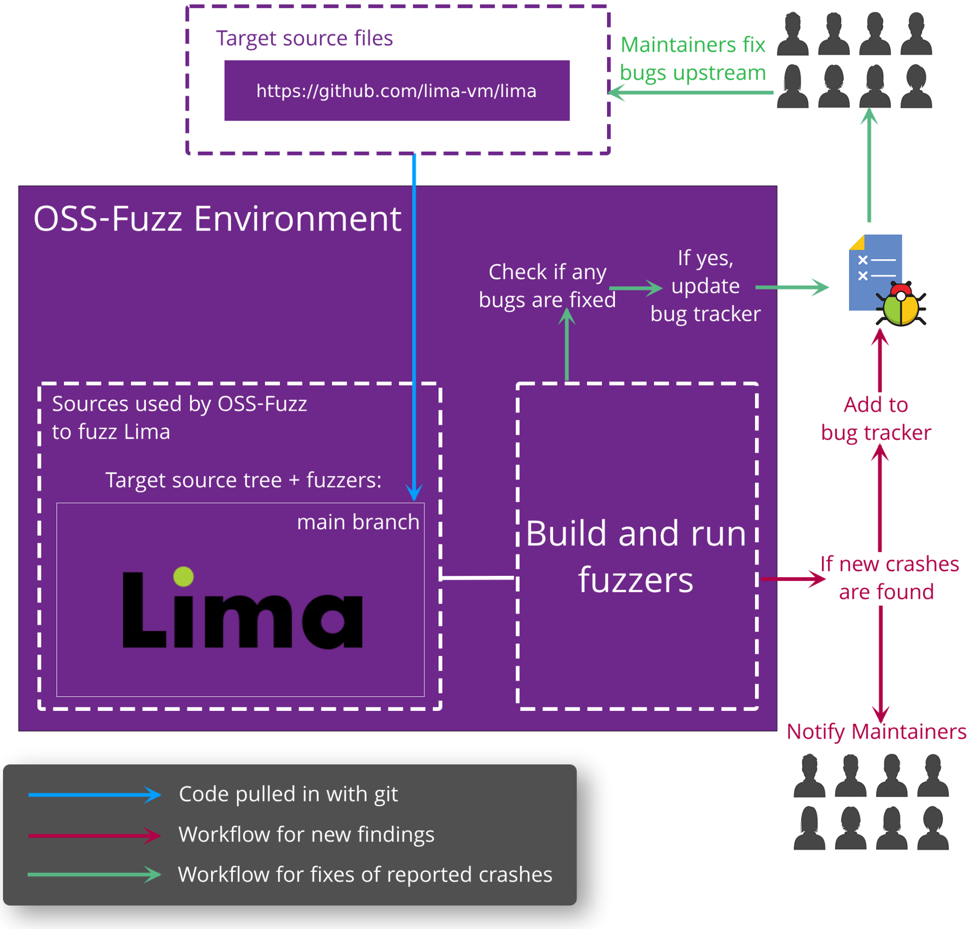
Target source files
https://github.com/lima-vm/lima
Maintainers fix bugs upstream
OSS-Fuzz Environment
Check if any bugs are fixed
If yes, update bug tracker
Sources used by OSS-Fuzz to fuzz Lima
Target source tree + fuzzers:
main branch
Lima
Build and run fuzzers
Add to bug tracker
If new crashes are found
Notify Maintainers
Code pulled in with git
Workflow for new findings
Workflow for fixes of reported crashes

Figure 1: Limas fuzzing architecture

A central component in the Limas fuzzing infrastructure is its integration into OSS-Fuzz. The Lima source code and Limas fuzz tests are the two core elements that OSS-Fuzz uses to fuzz Lima. The following diagram gives an overview of how OSS-Fuzz uses these two elements and what happens when an issue is found/fixed.

The current OSS-Fuzz set up builds the fuzzers by cloning the upstream Lima GitHub repository to get the latest Lima source code and its fuzz tests. OSS-Fuzz then builds the fuzzers against the cloned Lima source code which ensures that the fuzzers always run against the latest Lima commit.

This build cycle happens daily and OSS-Fuzz will verify if any existing bugs have been fixed. If OSS-fuzz finds that any bugs have been fixed OSS-Fuzz marks the crashes as fixed in the Monorail bug tracker and notifies maintainers.

In each fuzzing iteration, OSS-Fuzz uses its corpus accumulated from previous fuzz runs. If OSS-Fuzz detects any crashes when running the fuzzers, OSS-Fuzz performs the following actions:

1. A detailed crash report is created.
2. An issue in the Monorail bug tracker is created.
3. An email is sent to maintainers with links to the report and relevant entry in the bug tracker.

OSS-Fuzz has a 90 day disclosure policy, meaning that a bug becomes public in the bug tracker if it has not been fixed. The detailed report is never made public. The Lima maintainers will fix issues upstream, and OSS-Fuzz will pull the latest Lima master branch the next time it performs a fuzz run and verify that a given issue has been fixed.

Lima Fuzzers

In this section we present a highlight of the Lima fuzzers and which parts of Lima they test. In total, 8 fuzzers were written during the fuzzing audit. During the audit we focused primarily on testing APIs with a large callgraph and APIs that involve processing of input with an emphasis on complex processing.

The internals of Lima presented some challenges when it comes to fuzz testing. The main challenge is that Lima invokes other binaries on the system which takes execution off process. Fuzzing is currently done fully in-process, and in the context of OSS-Fuzz, Lima is not able to test execution paths that include invocation of binaries. To test these execution paths, Lima will need some restructuring of its internals which allow mocking the calls to the binaries.

All the fuzzers we wrote during the audit are checked into Limas upstream source tree.

#	Name	Lima Package
1	FuzzConvertToRaw	github.com/lima-vm/lima/pkg/nativeimgutil
2	FuzzDownload	github.com/lima-vm/lima/pkg/downloader
3	FuzzEvaluateExpression	github.com/lima-vm/lima/pkg/yqutil
4	FuzzInspect	github.com/lima-vm/lima/pkg/store
5	FuzzIsISO9660	github.com/lima-vm/lima/pkg/iso9660util

#	Name	Lima Package
6	FuzzLoadYAMLByFilePath	github.com/lima-vm/lima/pkg/store
7	FuzzParse	github.com/lima-vm/lima/pkg/guestagent/procnettcp
8	FuzzSetupEnv	github.com/lima-vm/lima/pkg/cidata

Issues found by fuzzers

During the audit, the fuzzers found 11 crashes. The majority of these crashes have their root cause in 3rd-party libraries. YAML-parsers in particular had multiple issues which have the ability to crash the process and exhaust memory of the machine.

Each of the found issues are reproducible from inside the OSS-Fuzz environment. For more details on reproducing issues found by OSS-Fuzz, see https://google.github.io/oss-fuzz/advanced-topics/reproducing/. We have been able to reproduce the issues outside of the OSS-Fuzz environment, and we have included these reproducers for each crash.

#	Name	Fixed
1	Stack overflow in 3rd-party yaml parser	No
2	Type confusion in 3rd-party yaml parser	No
3	Memory exhaustion in 3rd-party yaml parser	No
4	Index out of range panic in 3rd-party yaml parser	No
5	Slice bounds out of range in 3rd-party yaml parser	No
6	Integer underflow in 3rd-party yq library	No
7	Index out of range in 3rd-party yq library	No
8	Index out of range in 3rd-party yq library	No
9	Memory exhaustion when evaluating expression	No
10	Divide by zero panic	No
11	Length of string controllable by user input in 3rd-party yq library	No

Stack overflow in 3rd-party yaml parser

Severity	Low
Status	Reported
id	ADA-LIMA-FUZZ-2024-1
Affected Lima Component	github.com/lima-vm/lima/pkg/limayaml
OSS-Fuzz issue	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=70411

This is a stack overflow from high recursion controllable by the input. The issue exists in a 3rd-party YAML parser, and Lima can trigger the issue from `LoadYAMLByFilePath`.

Ada Logics have filed an issue with the 3rd-party dependency regarding this issue: https://github.com/goccy/go-yaml/issues/464

Reproducer

Lima commit: `6c2bfaa9197b54c8cc5a93707e65e22422b0616c`

`lima/pkg/store/instance_test.go`

```go
package store

import (
	"os"
	"path/filepath"
	"testing"
)

func TestLoadYAMLByFilePath(t *testing.T) {
	fileContents, err := os.ReadFile("testcase")
	if err != nil {
		panic(err)
	}
	localFile := filepath.Join(t.TempDir(), "yaml_file.yml")
	err := os.WriteFile(localFile, fileContents, 0o600)
	if err != nil {
		t.Fatal(err)
	}
	//nolint:errcheck // The test doesn't check the return value
	LoadYAMLByFilePath(localFile)
}
```

Stacktrace

```
	runtime: goroutine stack exceeds 1000000000-byte limit
runtime: sp=0x10c020270418 stack=[0x10c020270000, 0x10c040270000]
fatal error: stack overflow
runtime stack:
runtime.throw({0x55773d05cd10?, 0x200000001?})
	runtime/panic.go:1023 +0x5e fp=0x7ffea49ce9f0 sp=0x7ffea49ce9c0 pc=0x55773ca820de
runtime.newstack()
	runtime/stack.go:1103 +0x5bd fp=0x7ffea49ceba0 sp=0x7ffea49ce9f0 pc=0x55773ca9d59d
runtime.morestack()
	runtime/asm_amd64.s:616 +0x77 fp=0x7ffea49ceba8 sp=0x7ffea49ceba0 pc=0x55773cab4f17
goroutine 17 gp=0x10c000006700 m=1 mp=0x10c000054008 [running, locked to thread]:
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:263 +0x15f3 fp=0x10c020270428 sp=0x10c020270420 pc=0x55773ce5e953
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020270598 sp=0x10c020270428 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020270708 sp=0x10c020270598 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020270878 sp=0x10c020270708 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c0202709e8 sp=0x10c020270878 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020270b58 sp=0x10c0202709e8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020270cc8 sp=0x10c020270b58 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020270e38 sp=0x10c020270cc8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020270fa8 sp=0x10c020270e38 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020271118 sp=0x10c020270fa8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020271288 sp=0x10c020271118 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c0202713f8 sp=0x10c020271288 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020271568 sp=0x10c0202713f8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c0202716d8 sp=0x10c020271568 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020271848 sp=0x10c0202716d8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c0202719b8 sp=0x10c020271848 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020271b28 sp=0x10c0202719b8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020271c98 sp=0x10c020271b28 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020271e08 sp=0x10c020271c98 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
```

```
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020271f78 sp=0x10c020271e08 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c0202720e8 sp=0x10c020271f78 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020272258 sp=0x10c0202720e8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c0202723c8 sp=0x10c020272258 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020272538 sp=0x10c0202723c8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c0202726a8 sp=0x10c020272538 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020272818 sp=0x10c0202726a8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020272988 sp=0x10c020272818 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020272af8 sp=0x10c020272988 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020272c68 sp=0x10c020272af8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020272dd8 sp=0x10c020272c68 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020272f48 sp=0x10c020272dd8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c0202730b8 sp=0x10c020272f48 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020273228 sp=0x10c0202730b8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020273398 sp=0x10c020273228 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020273508 sp=0x10c020273398 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020273678 sp=0x10c020273508 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c0202737e8 sp=0x10c020273678 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020273958 sp=0x10c0202737e8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020273ac8 sp=0x10c020273958 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020273c38 sp=0x10c020273ac8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020273da8 sp=0x10c020273c38 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020273f18 sp=0x10c020273da8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020274088 sp=0x10c020273f18 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c0202741f8 sp=0x10c020274088 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
```

```
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020274368 sp=0x10c0202741f8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c0202744d8 sp=0x10c020274368 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020274648 sp=0x10c0202744d8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c0202747b8 sp=0x10c020274648 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020274928 sp=0x10c0202747b8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c020274a98 sp=0x10c020274928 pc=0x55773ce5e45a
...1458796 frames elided...
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026c748 sp=0x10c04026c5d8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026c8b8 sp=0x10c04026c748 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026ca28 sp=0x10c04026c8b8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026cb98 sp=0x10c04026ca28 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026cd08 sp=0x10c04026cb98 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026ce78 sp=0x10c04026cd08 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026cfe8 sp=0x10c04026ce78 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026d158 sp=0x10c04026cfe8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026d2c8 sp=0x10c04026d158 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026d438 sp=0x10c04026d2c8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026d5a8 sp=0x10c04026d438 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026d718 sp=0x10c04026d5a8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026d888 sp=0x10c04026d718 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026d9f8 sp=0x10c04026d888 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026db68 sp=0x10c04026d9f8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026dcd8 sp=0x10c04026db68 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026de48 sp=0x10c04026dcd8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026dfb8 sp=0x10c04026de48 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
	github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026e128 sp=0x10c04026dfb8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
```

```
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026e298 sp=0x10c04026e128 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026e408 sp=0x10c04026e298 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026e578 sp=0x10c04026e408 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026e6e8 sp=0x10c04026e578 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026e858 sp=0x10c04026e6e8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026e9c8 sp=0x10c04026e858 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3260})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026eb38 sp=0x10c04026e9c8 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0x10c000250000, {0x55773d1ef920, 0x10c0001d3480})
        github.com/goccy/go-yaml@v1.12.0/decode.go:308 +0x10fa fp=0x10c04026eca8 sp=0x10c04026eb38 pc=0x55773ce5e45a
github.com/goccy/go-yaml.(*Decoder).parse(0x10c000250000, {0x10c00024e2c0?, 0x55773d1ead20?, 0x10c000185b60?})
        github.com/goccy/go-yaml@v1.12.0/decode.go:1693 +0x1b2 fp=0x10c04026ed28 sp=0x10c04026eca8 pc=0x55773ce73992
github.com/goccy/go-yaml.(*Decoder).decodeInit(0x10c000250000)
        github.com/goccy/go-yaml@v1.12.0/decode.go:1714 +0x1d1 fp=0x10c04026ed78 sp=0x10c04026ed28 pc=0x55773ce73c91
github.com/goccy/go-yaml.(*Decoder).DecodeContext(0x10c000250000, {0x55773d1ec348, 0x55773deff9a0}, {0x55773d160600?, 0x10c0001d8508?})
        github.com/goccy/go-yaml@v1.12.0/decode.go:1762 +0x494 fp=0x10c04026ee28 sp=0x10c04026ed78 pc=0x55773ce74494
github.com/goccy/go-yaml.UnmarshalContext({0x55773d1ec348, 0x55773deff9a0}, {0x10c00024e000, 0x2b1, 0x2b2}, {0x55773d160600, 0x10c0001d8508}, {0x10c00017e5e0, 0x2, 0x2})
        github.com/goccy/go-yaml@v1.12.0/yaml.go:191 +0x23d fp=0x10c04026ee90 sp=0x10c04026ee28 pc=0x55773ce851dd
github.com/goccy/go-yaml.UnmarshalWithOptions(...)
        github.com/goccy/go-yaml@v1.12.0/yaml.go:185
github.com/lima-vm/lima/pkg/limayaml.unmarshalYAML({0x10c00024e000, 0x2b1, 0x2b2}, {0x55773d160600, 0x10c0001d8508}, {0x10c0001ded80, 0x31})
```

```
        github.com/lima-vm/lima/pkg/limayaml/load.go:37 +0x13b fp=0x10c04026f0c0 sp=0x10c04026ee90 pc=0x55773cf0d49b
github.com/lima-vm/lima/pkg/limayaml.Load({0x10c00024e000, 0x2b1, 0x2b2}, {0x10c00019faa0, 0x25})
        github.com/lima-vm/lima/pkg/limayaml/load.go:59 +0x129 fp=0x10c04026f208 sp=0x10c04026f0c0 pc=0x55773cf0de89
github.com/lima-vm/lima/pkg/store.LoadYAMLByFilePath({0x10c00019faa0?, 0x0?})
```

Type confusion in 3rd-party yaml parser

Severity	Low
Status	Reported
id	ADA-LIMA-FUZZ-2024-2
Affected Lima Component	github.com/lima-vm/lima/pkg/limayaml
OSS-Fuzz issue	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=70415

This is a type confusion - which Go panics with `panic: interface conversion:` - in a 3rd-party YAML parser. The issue is triggered from invoking `LoadYAMLByFilePath` with well-crafted YAML.

Reproducer

Lima commit: 6c2bfaa9197b54c8cc5a93707e65e22422b0616c

`lima/pkg/store/instance_test.go`

```go
package store

import (
    "os"
    "path/filepath"
    "testing"
)

func TestLoadYAMLByFilePath(t *testing.T) {
    b := []byte{32, 32, 32, 32, 32, 32, 32, 32, 33, 33, 98, 105, 110,
        97, 114, 121, 32, 32, 49, 55, 48, 49, 52, 49, 49, 56, 51, 52,
        54, 48, 52, 54, 57, 50, 51, 49, 55, 51, 49, 54, 56, 55, 51, 48,
        51, 55, 49, 53, 56, 56, 52, 49, 48, 53, 55, 50}
    localFile := filepath.Join(t.TempDir(), "yaml_file.yml")
    err := os.WriteFile(localFile, b, 0o600)
    if err != nil {
        t.Fatal(err)
    }
    //nolint:errcheck // The test doesn't check the return value
    LoadYAMLByFilePath(localFile)
}
```

Stacktrace

```
--- FAIL: TestLoadYAMLByFilePath (0.00s)
panic: interface conversion: interface {} is uint64, not string [recovered]
	panic: interface conversion: interface {} is uint64, not string

goroutine 6 [running]:
testing.tRunner.func1.2({0x93c040, 0xc0001ac120})
	/usr/lib/go-1.22/src/testing/testing.go:1631 +0x24a
testing.tRunner.func1()
	/usr/lib/go-1.22/src/testing/testing.go:1634 +0x377
panic({0x93c040?, 0xc0001ac120?})
	/usr/lib/go-1.22/src/runtime/panic.go:770 +0x132
github.com/goccy/go-yaml.(*Decoder).nodeToValue(0xc0000000c0, {0xa9fb80, 0xc00007a560})
	/home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/decode.go:293 +0xc4c
github.com/goccy/go-yaml.(*Decoder).parse(0xc0000000c0, {0xc00002eb80?, 0xa97a80?, 0xc00010bef0?})
	/home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/decode.go:1693 +0xe5
github.com/goccy/go-yaml.(*Decoder).decodeInit(0xc0000000c0)
	/home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/decode.go:1714 +0xb1
github.com/goccy/go-yaml.(*Decoder).DecodeContext(0xc0000000c0, {0xa9b220, 0xe6f840}, {0x8ff080?, 0xc000142508?})
	/home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/decode.go:1762 +0x19a
github.com/goccy/go-yaml.UnmarshalContext({0xa9b220, 0xe6f840}, {0xc0001aa000, 0x38, 0x200}, {0x8ff080, 0xc000142508}, {0xc0000387b0, 0x2, 0x2})
	/home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/yaml.go:191 +0x225
github.com/goccy/go-yaml.UnmarshalWithOptions(...)
	/home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/yaml.go:185
github.com/lima-vm/lima/pkg/limayaml.unmarshalYAML({0xc0001aa000, 0x38, 0x200}, {0x8ff080, 0xc000142508}, {0xc0001741e0, 0x43})
	/tmp/lima/pkg/limayaml/load.go:37 +0x11b
github.com/lima-vm/lima/pkg/limayaml.Load({0xc0001aa000, 0x38, 0x200}, {0xc00002eac0, 0x37})
	/tmp/lima/pkg/limayaml/load.go:59 +0x109
github.com/lima-vm/lima/pkg/store.LoadYAMLByFilePath({0xc00002eac0?, 0xdcb900?})
	/tmp/lima/pkg/store/store.go:127 +0x48
github.com/lima-vm/lima/pkg/store.TestLoadYAMLByFilePath(0xc000138ea0)
	/tmp/lima/pkg/store/instance_test.go:17 +0x167
testing.tRunner(0xc000138ea0, 0xa049a0)
	/usr/lib/go-1.22/src/testing/testing.go:1689 +0xfb
created by testing.(*T).Run in goroutine 1
```

```
        /usr/lib/go-1.22/src/testing/testing.go:1742 +0x390
exit status 2
FAIL    github.com/lima-vm/lima/pkg/store       0.012s
```

Memory exhaustion in 3rd-party yaml parser

Severity	Low
Status	Reported
id	ADA-LIMA-FUZZ-2024-3
Affected Lima Component	github.com/lima-vm/lima/pkg/limayaml
OSS-Fuzz issue	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=70393

A fuzzer was able to invoke `LoadYAMLByFilePath` and cause the system to exhaust memory. As such, this crash can affect other services on the machine negatively and result in denial of service.

They may be related to https://github.com/goccy/go-yaml/issues/461.

Reproducer

Lima commit: `6c2bfaa9197b54c8cc5a93707e65e22422b0616c`

`lima/pkg/store/instance_test.go`

Open a pane with `top` to observe memory usage.
Download the testcase from here: https://oss-fuzz.com/testcase-detail/4888408376279040 and name it `"seed"` in the same directory as the reproducer. Note that the testcase is only 87 KB.

Run the following unit test:

```go
package store

import (
    "os"
    "path/filepath"
    "testing"
)

func TestLoadYAMLByFilePath(t *testing.T) {
    b, err := os.ReadFile("seed")
    if err != nil {
        panic(err)
    }
    b = append(b, b...)
    localFile := filepath.Join(t.TempDir(), "yaml_file.yml")
    err = os.WriteFile(localFile, b, 0o600)
    if err != nil {
        t.Fatal(err)
    }
    LoadYAMLByFilePath(localFile)
}
```

The memory will now start to creep and depending on the system resources the machine will be denied of service from a memory exhaustion.

Index out of range panic in 3rd-party yaml parser

Severity	Low
Status	Reported
id	ADA-LIMA-FUZZ-2024-4
Affected Lima Component	github.com/lima-vm/lima/pkg/limayaml
OSS-Fuzz issue	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=70404

This is an issue with minor severity in a production context. A short YAML string can trigger an index out of range panic in a 3rd-party YAML parser. Ada Logics submitted a fix for this crash but the project has not responded to it at the time of writing.

Reproducer

Lima commit: 6c2bfaa9197b54c8cc5a93707e65e22422b0616c

lima/pkg/store/instance_test.go

```
package store

import (
        "os"
        "path/filepath"
        "testing"
)

func TestLoadYAMLByFilePath(t *testing.T) {
        b := []byte{48,95}
        localFile := filepath.Join(t.TempDir(), "yaml_file.yml")
        err := os.WriteFile(localFile, b, 0o600)
        if err != nil {
                t.Fatal(err)
        }
        LoadYAMLByFilePath(localFile)
}
```

Stacktrace

```
--- FAIL: TestLoadYAMLByFilePath (0.00s)
panic: runtime error: index out of range [1] with length 1 [recovered]
        panic: runtime error: index out of range [1] with length 1

goroutine 21 [running]:
testing.tRunner.func1.2({0x98db00, 0xc0000da348})
        /usr/lib/go-1.22/src/testing/testing.go:1631 +0x24a
testing.tRunner.func1()
        /usr/lib/go-1.22/src/testing/testing.go:1634 +0x377
panic({0x98db00?, 0xc0000da348?})
        /usr/lib/go-1.22/src/runtime/panic.go:770 +0x132
github.com/goccy/go-yaml/ast.Integer(0xc0000ae5a0)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/ast/ast.go:336 +0x9d2
github.com/goccy/go-yaml/parser.(*parser).parseScalarValue(0x7f7c4d043e88?, 0xc0000ae5a0)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/parser/parser.go:470 +0x48e
github.com/goccy/go-yaml/parser.(*parser).parseScalarValueWithComment(0xc00011d8e0, 0xc0000aaf80, 0x0?)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/parser/parser.go:443 +0x25
github.com/goccy/go-yaml/parser.(*parser).createNodeFromToken(0xc00011d8e0, 0xc0000aaf80, 0xc0000ae5a0)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/parser/parser.go:650 +0x4a
github.com/goccy/go-yaml/parser.(*parser).parseToken(0xe6f840?, 0xc0000aaf80, 0x0?)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/parser/parser.go:632 +0x1c
github.com/goccy/go-yaml/parser.(*parser).parse(0xc00011d8e0, {0xc0000ba118?, 0x1?, 0x0?}, 0x0?)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/parser/parser.go:688 +0x14d
github.com/goccy/go-yaml/parser.Parse({0xc0000ba118?, 0xc000108ac0?, 0x2?}, 0x7f7c4d0561d8?)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/parser/parser.go:724 +0x29
github.com/goccy/go-yaml/parser.ParseBytes({0xc000108ac0?, 0xc0000bfef0?, 0xa97700?}, 0x0)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/parser/parser.go:714 +0x3d
github.com/goccy/go-yaml.(*Decoder).parse(0xc00017e000, {0xc000108ac0?, 0xa97a80?, 0xc0000bfef0?})
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/decode.go:1686 +0x3e
github.com/goccy/go-yaml.(*Decoder).decodeInit(0xc00017e000)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/decode.go:1714 +0xb1
```

```
github.com/goccy/go-yaml.(*Decoder).DecodeContext(0xc00017e000, {0xa9b220, 0xe6f840}, {0x8ff080?, 0xc000102508?})
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/decode.go:1762 +0x19a
github.com/goccy/go-yaml.UnmarshalContext({0xa9b220, 0xe6f840}, {0xc00017c000, 0x2, 0x200}, {0x8ff080, 0xc000102508}, {0xc0000a8790, 0x2, 0x2})
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/yaml.go:191 +0x225
github.com/goccy/go-yaml.UnmarshalWithOptions(...)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/yaml.go:185
github.com/lima-vm/lima/pkg/limayaml.unmarshalYAML({0xc00017c000, 0x2, 0x200}, {0x8ff080, 0xc000102508}, {0xc0001381e0, 0x42})
        /tmp/lima/pkg/limayaml/load.go:37 +0x11b
github.com/lima-vm/lima/pkg/limayaml.Load({0xc00017c000, 0x2, 0x200}, {0xc000108a00, 0x36})
        /tmp/lima/pkg/limayaml/load.go:59 +0x109
github.com/lima-vm/lima/pkg/store.LoadYAMLByFilePath({0xc000108a00?, 0xb4e594?})
        /tmp/lima/pkg/store/store.go:127 +0x48
github.com/lima-vm/lima/pkg/store.TestLoadYAMLByFilePath(0xc0000f7040)
        /tmp/lima/pkg/store/instance_test.go:17 +0xd4
testing.tRunner(0xc0000f7040, 0xa049a0)
        /usr/lib/go-1.22/src/testing/testing.go:1689 +0xfb
created by testing.(*T).Run in goroutine 1
        /usr/lib/go-1.22/src/testing/testing.go:1742 +0x390
exit status 2
FAIL    github.com/lima-vm/lima/pkg/store       0.014s
```

Slice bounds out of range in 3rd-party yaml parser

Severity	Low
Status	Reported
id	ADA-LIMA-FUZZ-2024-5
Affected Lima Component	github.com/lima-vm/lima/pkg/limayaml
OSS-Fuzz issue	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=70394

This is a minor issue in a 3rd-party YAML parser which a fuzzer was able to trigger by invoking Limas `LoadYAMLByFilePath`.

Reproducer

Lima commit: 6c2bfaa9197b54c8cc5a93707e65e22422b0616c

`lima/pkg/store/instance_test.go`

```go
package store

import (
    "os"
    "path/filepath"
    "testing"
)

func TestLoadYAMLByFilePath(t *testing.T) {
    b := []byte{62,62,62,62,62,35,62,140,255,1,13,83,33,32}
    localFile := filepath.Join(t.TempDir(), "yaml_file.yml")
    err := os.WriteFile(localFile, b, 0o600)
    if err != nil {
            t.Fatal(err)
    }
    LoadYAMLByFilePath(localFile)
}
```

Stacktrace

```
--- FAIL: TestLoadYAMLByFilePath (0.00s)
panic: runtime error: slice bounds out of range [:-2] [recovered]
        panic: runtime error: slice bounds out of range [:-2]

goroutine 19 [running]:
testing.tRunner.func1.2({0x98db00, 0xc0000d6348})
        /usr/lib/go-1.22/src/testing/testing.go:1631 +0x24a
testing.tRunner.func1()
        /usr/lib/go-1.22/src/testing/testing.go:1634 +0x377
panic({0x98db00?, 0xc0000d6348?})
        /usr/lib/go-1.22/src/runtime/panic.go:770 +0x132
github.com/goccy/go-yaml/scanner.(*Scanner).scanLiteralHeader(0xc00011d840, 0xc0000bb9a0)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/scanner/scanner.go:574 +0x1278
github.com/goccy/go-yaml/scanner.(*Scanner).scan(0xc00011d840, 0xc0000bb9a0)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/scanner/scanner.go:774 +0x186e
github.com/goccy/go-yaml/scanner.(*Scanner).Scan(0xc00011d840)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/scanner/scanner.go:898 +0xdf
github.com/goccy/go-yaml/lexer.Tokenize({0xc000072920?, 0xc000108ac0?})
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/lexer/lexer.go:16 +0xf1
github.com/goccy/go-yaml/parser.ParseBytes({0xc000108ac0?, 0xc0000b7ef0?, 0xa97700?}, 0x0)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/parser/parser.go:713 +0x30
github.com/goccy/go-yaml.(*Decoder).parse(0xc00017e000, {0xc000108ac0?, 0xa97a80?, 0xc0000b7ef0?})
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/decode.go:1686 +0x3e
github.com/goccy/go-yaml.(*Decoder).decodeInit(0xc00017e000)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/decode.go:1714 +0xb1
github.com/goccy/go-yaml.(*Decoder).DecodeContext(0xc00017e000, {0xa9b220, 0xe6f840}, {0x8ff080?, 0xc000102508?})
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/decode.go:1762 +0x19a
github.com/goccy/go-yaml.UnmarshalContext({0xa9b220, 0xe6f840}, {0xc00017c000, 0xe, 0x200}, {0x8ff080, 0xc000102508}, {0xc0000b0770, 0x2, 0x2})
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/yaml.go:191 +0x225
github.com/goccy/go-yaml.UnmarshalWithOptions(...)
        /home/adam/go/pkg/mod/github.com/goccy/go-yaml@v1.12.0/yaml.go:185
github.com/lima-vm/lima/pkg/limayaml.unmarshalYAML({0xc00017c000, 0xe, 0x200}, {0x8ff080, 0xc000102508}, {0xc0001381e0, 0x42})
```

```
        /tmp/lima/pkg/limayaml/load.go:37 +0x11b
github.com/lima-vm/lima/pkg/limayaml.Load({0xc00017c000, 0xe, 0x200}, {0xc000108a00, 0x36})
        /tmp/lima/pkg/limayaml/load.go:59 +0x109
github.com/lima-vm/lima/pkg/store.LoadYAMLByFilePath({0xc000108a00?, 0xf?})
        /tmp/lima/pkg/store/store.go:127 +0x48
github.com/lima-vm/lima/pkg/store.TestLoadYAMLByFilePath(0xc0000f3040)
        /tmp/lima/pkg/store/instance_test.go:17 +0xf9
testing.tRunner(0xc0000f3040, 0xa049a0)
        /usr/lib/go-1.22/src/testing/testing.go:1689 +0xfb
created by testing.(*T).Run in goroutine 1
        /usr/lib/go-1.22/src/testing/testing.go:1742 +0x390
exit status 2
FAIL    github.com/lima-vm/lima/pkg/store       0.017s
```

Integer underflow in 3rd-party yq library

Severity	Low
Status	Reported
id	ADA-LIMA-FUZZ-2024-6
Affected Lima Component	github.com/lima-vm/lima/pkg/yqutil
OSS-Fuzz issue	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=70712

This is an issue in a 3rd-party YAML parser which a fuzzer was able to trigger by invoking `EvaluateExpression`. The fuzzer is able to control the second parameter to `strings.Repeat()` which is the number of times a string should be repeated. The fuzzer was able to place a negative value in that call which is not allowed.

Another fuzzer found a similar issue (https://oss-fuzz.com/testcase-detail/4578834622513152) where it was able to place a high value in the same call to `strings.Repeat()` which will crash Lima with an Out-of-Memory panic.

Reproducer

Lima commit: 6c2bfaa9197b54c8cc5a93707e65e22422b0616c

`lima/pkg/yqutil/yqutil_test.go`

```
func TestEvaluateExpressionPoc(t *testing.T) {
        expression := `"4"%8%-444444*=4444444444*=4444444`
        content := []byte{52, 52, 52, 52, 52, 56, 37, 37, 52, 52, 52,
            52, 52, 52, 42, 61, 52, 52, 52, 52, 52, 52, 52, 52, 52, 52,
            42, 61, 52, 52, 52, 52, 52, 54, 52, 52, 44, 49, 33, 33, 98,
            52, 52, 52, 42, 61, 52, 52, 52, 52, 52, 52, 52, 52}
        _, _ = EvaluateExpression(expression, content)
}
```

Stacktrace

```
--- FAIL: TestEvaluateExpressionPoc (0.00s)
panic: strings: negative Repeat count [recovered]
```

```
        panic: strings: negative Repeat count

goroutine 19 [running]:
testing.tRunner.func1.2({0x8fe120, 0xa68900})
        /usr/lib/go-1.22/src/testing/testing.go:1631 +0x24a
testing.tRunner.func1()
        /usr/lib/go-1.22/src/testing/testing.go:1634 +0x377
panic({0x8fe120?, 0xa68900?})
        /usr/lib/go-1.22/src/runtime/panic.go:770 +0x132
strings.Repeat({0xc00018cd40?, 0xc000204700?}, 0xc000277ae0?)
        /usr/lib/go-1.22/src/strings/strings.go:549 +0x318
github.com/mikefarah/yq/v4/pkg/yqlib.repeatString(0x7e0017?, 0xc1a46f916cc5fb97?)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_multiply.go:157 +0x94
github.com/mikefarah/yq/v4/pkg/yqlib.multiplyScalars(0xc000204a80, 0xc000204700)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_multiply.go:95 +0x208
github.com/mikefarah/yq/v4/pkg/yqlib.multiplyOperator.multiply.func1(0xeb0180, {0xc0002c6a50, 0xc0002c6ab0, 0x1, {0x0, 0x0}}, 0xc000204a80, 0xc000204700)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_multiply.go:76 +0x3e5
github.com/mikefarah/yq/v4/pkg/yqlib.resultsForRHS(0xeb0180, {0xc0002c6a50, 0xc0002c6ab0, 0x1, {0x0, 0x0}}, 0xc000204a80, {0x0, 0x0, 0xc000278130}, ...)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:94 +0x61a
github.com/mikefarah/yq/v4/pkg/yqlib.doCrossFunc(0xeb0180, {0xc0002c6a50, 0xc0002c6ab0, 0x1, {0x0, 0x0}}, 0xc0000b45b8, {0x0, 0x0, 0xc000278130})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:131 +0x408
github.com/mikefarah/yq/v4/pkg/yqlib.crossFunctionWithPrefs(0xeb0180, {0xc0002c68d0, 0xc0002c6930, 0x1, {0x0, 0x0}}, 0xc0000b45b8, {0x0, 0x0, 0xc000278130})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:164 +0x398
github.com/mikefarah/yq/v4/pkg/yqlib.crossFunction(0xc0000b79e0?, {0xc0002c68d0, 0xc0002c6930, 0x1, {0x0, 0x0}}, 0x0?, 0xc0002d0240?, 0x80?)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:142 +0x93
github.com/mikefarah/yq/v4/pkg/yqlib.multiplyOperator(0xeb0180, {0xc0002c68d0, 0xc0002c6930, 0x1, {0x0, 0x0}}, 0xc0000b45b8)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_multiply.go:33 +0x158
github.com/mikefarah/yq/v4/pkg/yqlib.(*dataTreeNavigator).GetMatchingNodes(0xeb0180, {0xc0002c68d0, 0xc0002c6930, 0x1, {0x0, 0x0}}, 0xc0000b45b8)
```

```
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/data_tree_navigator.go:65 +0x21f
github.com/mikefarah/yq/v4/pkg/yqlib.resultsForRHS(0xeb0180, {0xc0002c68d0, 0xc0002c6930, 0x1, {0x0, 0x0}}, 0xc0002049a0, {0x0, 0x0, 0xc000278758}, ...)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:73 +0x210
github.com/mikefarah/yq/v4/pkg/yqlib.doCrossFunc(0xeb0180, {0xc0002c68d0, 0xc0002c6930, 0x1, {0x0, 0x0}}, 0xc0000b45d0, {0x0, 0x0, 0xc000278758})
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:131 +0x408
github.com/mikefarah/yq/v4/pkg/yqlib.crossFunctionWithPrefs(0xeb0180, {0xc0002c6600, 0xc0002c6870, 0x1, {0x0, 0x0}}, 0xc0000b45d0, {0x0, 0x0, 0xc000278758})
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:164 +0x398
github.com/mikefarah/yq/v4/pkg/yqlib.crossFunction(0xc000278958?, {0xc0002c6600, 0xc0002c6870, 0x1, {0x0, 0x0}}, 0x1?, 0x10?, 0x10?)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:142 +0x93
github.com/mikefarah/yq/v4/pkg/yqlib.assignUpdateOperator(0xeb0180, {0xc0002c6600, 0xc0002c6660, 0x1, {0x0, 0x0}}, 0xc0000b45d0)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_assign.go:44 +0x429
github.com/mikefarah/yq/v4/pkg/yqlib.(*dataTreeNavigator).GetMatchingNodes(0xeb0180, {0xc0002c6600, 0xc0002c6660, 0x1, {0x0, 0x0}}, 0xc0000b45d0)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/data_tree_navigator.go:65 +0x21f
github.com/mikefarah/yq/v4/pkg/yqlib.compoundAssignFunction(0xeb0180, {0xc0002c6600, 0xc0002c6660, 0x1, {0x0, 0x0}}, 0xc0000b4540, 0xc000278bb8)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:46 +0x44d
github.com/mikefarah/yq/v4/pkg/yqlib.multiplyAssignOperator(0xc0000b79e0?, {0xc0002c6600, 0xc0002c6660, 0x1, {0x0, 0x0}}, 0x0?)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_multiply.go:28 +0xc8
github.com/mikefarah/yq/v4/pkg/yqlib.(*dataTreeNavigator).GetMatchingNodes(0xeb0180, {0xc0002c6600, 0xc0002c6660, 0x1, {0x0, 0x0}}, 0xc0000b4540)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/data_tree_navigator.go:65 +0x21f
github.com/mikefarah/yq/v4/pkg/yqlib.resultsForRHS(0xeb0180, {0xc0002c6600, 0xc0002c6660, 0x1, {0x0, 0x0}}, 0xc0002048c0, {0x0, 0x0, 0x9d1750}, ...)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:73 +0x210
github.com/mikefarah/yq/v4/pkg/yqlib.doCrossFunc(0xeb0180, {0xc0002c6600, 0xc0002c6660, 0x1, {0x0, 0x0}}, 0xc0000b4558, {0x0, 0x0
, 0x9d1750})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:131 +0x408
github.com/mikefarah/yq/v4/pkg/yqlib.crossFunctionWithPrefs(0xeb0180, {0xc0002c63c0, 0xc0002c65a0, 0x1, {0x0, 0x0}}, 0xc0000b4558, {0x0, 0x0, 0x9d1750})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:164 +0x398
github.com/mikefarah/yq/v4/pkg/yqlib.crossFunction(0xc000279260?, {0xc0002c63c0, 0xc0002c65a0, 0x1, {0x0, 0x0}}, 0x0?, 0x413e05?, 0x10?)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:142 +0x93
github.com/mikefarah/yq/v4/pkg/yqlib.moduloOperator(0xeb0180, {0xc0002c63c0, 0xc0002c6420, 0x1, {0x0, 0x0}}, 0xc0000b4558)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_modulo.go:13 +0x165
github.com/mikefarah/yq/v4/pkg/yqlib.(*dataTreeNavigator).GetMatchingNodes(0xeb0180, {0xc0002c63c0, 0xc0002c6420, 0x1, {0x0, 0x0}}, 0xc0000b4558)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/data_tree_navigator.go:65 +0x21f
github.com/mikefarah/yq/v4/pkg/yqlib.resultsForRHS(0xeb0180, {0xc0002c63c0, 0xc0002c6420, 0x1, {0x0, 0x0}}, 0xc0002047e0, {0x0, 0x0, 0x9d1750}, ...)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:73 +0x210
github.com/mikefarah/yq/v4/pkg/yqlib.doCrossFunc(0xeb0180, {0xc0002c63c0, 0xc0002c6420, 0x1, {0x0, 0x0}}, 0xc0000b4570, {0x0, 0x0, 0x9d1750})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:131 +0x408
github.com/mikefarah/yq/v4/pkg/yqlib.crossFunctionWithPrefs(0xeb0180, {0xc0002c6300, 0xc0002c6360, 0x1, {0x0, 0x0}}, 0xc0000b4570, {0x0, 0x0, 0x9d1750})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:164 +0x398
github.com/mikefarah/yq/v4/pkg/yqlib.crossFunction(0xc0002798d8?, {0xc0002c6300, 0xc0002c6360, 0x1, {0x0, 0x0}}, 0x0?, 0x413e05?, 0x10?)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:142 +0x93
github.com/mikefarah/yq/v4/pkg/yqlib.moduloOperator(0xeb0180, {0xc0002c6300, 0x0, 0x0, {0x0, 0x0}}, 0xc0000b4570)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_modulo.go:13 +0x165
github.com/mikefarah/yq/v4/pkg/yqlib.(*dataTreeNavigator).GetMatchingNodes(0xeb0180, {0xc0002c6300, 0x0, 0x0, {0x0, 0x0}}, 0xc0000b4570)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/data_tree_navigator.go:65 +0x21f
github.com/mikefarah/yq/v4/pkg/yqlib.(*streamEvaluator).Evaluate(0xc000279e28, {0xc0000f23e0, 0x1c}, {0xa6a4a0?, 0xc0000c6420?}, 0
xc0000b4570, {0xa6e348, 0xc0002ac3f0}, {0xa6b4b8, 0xc0002ac460})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/stream_evaluator.go:101 +0x2cc
github.com/mikefarah/yq/v4/pkg/yqlib.(*streamEvaluator).EvaluateFiles(0xc000279e28, {0x9a5f7f, 0x22}, {0xc000279e18, 0x1, 0x0?}, {0xa6e348, 0xc0002ac3f0}, {0xa6b4b8, 0xc0002ac460})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/stream_evaluator.go:58 +0x158
github.com/lima-vm/lima/pkg/yqutil.EvaluateExpression({0x9a5f7f, 0x22}, {0xc000072f2a, 0x36, 0x36})
        /tmp/lima/pkg/yqutil/yqutil.go:47 +0x796
github.com/lima-vm/lima/pkg/yqutil.TestEvaluateExpressionPoc(0xc0000fb860?)
        /tmp/lima/pkg/yqutil/yqutil_test.go:12 +0xb1
testing.tRunner(0xc0000fb860, 0x9d0b70)
        /usr/lib/go-1.22/src/testing/testing.go:1689 +0xfb
created by testing.(*T).Run in goroutine 1
        /usr/lib/go-1.22/src/testing/testing.go:1742 +0x390
exit status 2
FAIL    github.com/lima-vm/lima/pkg/yqutil      0.023s
```

Index out of range in 3rd-party yq library

Severity	Low
Status	Reported
id	ADA-LIMA-FUZZ-2024-7
Affected Lima Component	github.com/lima-vm/lima/pkg/yqutil
OSS-Fuzz issue	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=70614

This is a minor issue in a 3rd-party YAML parser. The fuzzer is able to trigger a call to the −1 index of a slice which results in panic.

Reproducer

Lima commit: 6c2bfaa9197b54c8cc5a93707e65e22422b0616c
lima/pkg/yqutil/yqutil_test.go

```go
func TestEvaluateExpressionPoc(t *testing.T) {
        expression := `:`
        content := []byte{}
        _, _ = EvaluateExpression(expression, content)
}
```

Stacktrace

```
--- FAIL: TestEvaluateExpressionPoc (0.00s)
panic: runtime error: index out of range [-1] [recovered]
        panic: runtime error: index out of range [-1]

goroutine 19 [running]:
testing.tRunner.func1.2({0x9691e0, 0xc0001ec4b0})
        /usr/lib/go-1.22/src/testing/testing.go:1631 +0x24a
testing.tRunner.func1()
        /usr/lib/go-1.22/src/testing/testing.go:1634 +0x377
panic({0x9691e0?, 0xc0001ec4b0?})
        /usr/lib/go-1.22/src/runtime/panic.go:770 +0x132
github.com/mikefarah/yq/v4/pkg/yqlib.handleToken({0xc0000b25f8, 0x1, 0x1?}, 0x0, {0xeb0180, 0x0, 0x0})
```

```
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/lexer.go:129 +0xf0a
github.com/mikefarah/yq/v4/pkg/yqlib.postProcessTokens({0xc0000b25f8, 0x1, 0x1})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/lexer.go:92 +0x55
github.com/mikefarah/yq/v4/pkg/yqlib.(*participleLexer).Tokenise(0xc0000b79e0?, {0xa65fb0?, 0x99e77a?})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/lexer_participle.go:592 +0x291
github.com/mikefarah/yq/v4/pkg/yqlib.(*expressionParserImpl).ParseExpression(0xc00028e940, {0xa65fb0, 0x1})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/expression_parser.go:29 +0xba
github.com/mikefarah/yq/v4/pkg/yqlib.(*streamEvaluator).EvaluateFiles(0xc000279e60, {0xa65fb0, 0x1}, {0xc000279e50, 0x1, 0x0?}, {0xa6e328, 0xc0002ac3f0}, {0xa6b498, 0xc0002ac460})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/stream_evaluator.go:47 +0x69
github.com/lima-vm/lima/pkg/yqutil.EvaluateExpression({0xa65fb0, 0x1}, {0xc000072f60, 0x0, 0x0})
        /tmp/lima/pkg/yqutil/yqutil.go:47 +0x796
github.com/lima-vm/lima/pkg/yqutil.TestEvaluateExpressionPoc(0xc0000fb860?)
        /tmp/lima/pkg/yqutil/yqutil_test.go:12 +0x29
testing.tRunner(0xc0000fb860, 0x9d0b50)
        /usr/lib/go-1.22/src/testing/testing.go:1689 +0xfb
created by testing.(*T).Run in goroutine 1
        /usr/lib/go-1.22/src/testing/testing.go:1742 +0x390
exit status 2
FAIL    github.com/lima-vm/lima/pkg/yqutil      0.022s
```

Index out of range in 3rd-party yq library

Severity	Low
Status	Reported
id	ADA-LIMA-FUZZ-2024-8
Affected Lima Component	github.com/lima-vm/lima/pkg/yqutil
OSS-Fuzz issue	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=70940

This is a minor issue in a 3rd-party YAML parser which the fuzzer is able to trigger by called `EvaluateExpression`. The fuzzer is able to trigger a read from a slice at an index that is not available.

Reproducer

Lima commit: 6c2bfaa9197b54c8cc5a93707e65e22422b0616c

lima/pkg/yqutil/yqutil_test.go

```go
func TestEvaluateExpressionPoc(t *testing.T) {
    expression := string([]byte{46,13,13})
    content := []byte{13, 63, 13, 13, 13, 13, 13, 13, 45, 45, 45, 10,
       13, 52, 13, 13, 51, 51, 51, 51, 51, 51, 51, 51, 51, 51, 51, 51,
       51, 51, 51, 51, 51, 13, 13, 13, 13, 13, 13, 13, 63, 13, 13, 13,
       13, 13, 13, 45, 45, 45, 64, 13, 122, 45, 46, 45, 10, 13, 13, 13,
        13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 63, 13, 13,
        13, 13, 13, 13, 45, 45, 45, 10, 13, 13, 13, 13, 114, 100, 48,
       13, 13, 13, 13, 63, 13, 13, 13, 13, 13, 13, 45, 45, 45, 10, 13,
       13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 63,
       13, 13, 13, 13, 13, 13, 45, 45, 45, 10, 33, 33, 110, 117, 108,
       108, 13, 13, 13, 13, 13, 35, 45, 51, 10, 51, 45, 45, 10, 13, 13,
        13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 63, 13,
        13, 13, 13, 13, 13, 45, 45, 45, 10, 13, 13, 13, 63, 13, 13, 13,
        13, 13, 13, 45, 45, 45, 13, 13, 45, 45, 45, 64, 13, 122, 45,
       46, 45, 10, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13,
       13, 13, 13, 63, 13, 13, 13, 13, 13, 13, 45, 45, 45, 10, 13, 13,
       13, 13, 114, 100, 48, 13, 13, 13, 13, 63, 13, 13, 13, 13, 13,
       13, 45, 45, 45, 10, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13,
       13, 13, 13, 13, 13, 63, 13, 13, 13, 13, 13, 13, 45, 45, 45, 10,
       33, 33, 110, 117, 108, 108, 13, 13, 45}
    _, _ = EvaluateExpression(expression, content)
}
```

Stacktrace

```
--- FAIL: TestEvaluateExpressionPoc (0.00s)
panic: runtime error: index out of range [1] with length 1 [recovered]
	panic: runtime error: index out of range [1] with length 1

goroutine 19 [running]:
testing.tRunner.func1.2({0x9691e0, 0xc0001ec630})
	/usr/lib/go-1.22/src/testing/testing.go:1631 +0x24a
testing.tRunner.func1()
	/usr/lib/go-1.22/src/testing/testing.go:1634 +0x377
panic({0x9691e0?, 0xc0001ec630?})
	/usr/lib/go-1.22/src/runtime/panic.go:770 +0x132
github.com/mikefarah/yq/v4/pkg/yqlib.doTraverseMap(0xc000279640, 0xc0002795f8?, {0xc0000c1319, 0x2}, {0x0, 0x0, 0x0, 0x0, 0x0}, 0x0)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_traverse_path.go:269 +0x334
github.com/mikefarah/yq/v4/pkg/yqlib.traverseMap({0xc0002c7470, 0x0, 0x0, {0x0, 0x0}}, 0xc0002d8460, 0xc0002d8700, {0x0, 0x0, 0x0, ...}, ...)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_traverse_path.go:223 +0xe7
github.com/mikefarah/yq/v4/pkg/yqlib.traverse({0xc0002c7470, 0x0, 0x0, {0x0, 0x0}}, 0xc0002d8460, 0xc00026d7c0)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_traverse_path.go:57 +0x4e7
github.com/mikefarah/yq/v4/pkg/yqlib.traversePathOperator(0xc0000b79e0?, {0xc0002c7470, 0x0, 0x0, {0x0, 0x0}}, 0xc0000b44b0)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_traverse_path.go:27 +0x145
github.com/mikefarah/yq/v4/pkg/yqlib.(*dataTreeNavigator).GetMatchingNodes(0xeb0180, {0xc0002c7470, 0x0, 0x0, {0x0, 0x0}}, 0xc0000b44b0)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/data_tree_navigator.go:65 +0x21f
github.com/mikefarah/yq/v4/pkg/yqlib.(*streamEvaluator).Evaluate(0xc000279d38, {0xc0000f23e0, 0x1c}, {0xa6a480?, 0xc0000c6420?}, 0xc0000b44b0, {0xa6e328, 0xc0002ac3f0}, {0xa6b498, 0xc0002ac460})
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/stream_evaluator.go:101 +0x2cc
github.com/mikefarah/yq/v4/pkg/yqlib.(*streamEvaluator).EvaluateFiles(0xc000279d38, {0xc0000c1318, 0x3}, {0xc000279d28, 0x1, 0x10?}, {0xa6e328, 0xc0002ac3f0}, {0xa6b498, 0xc0002ac460})
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/stream_evaluator.go:58 +0x158
github.com/lima-vm/lima/pkg/yqutil.EvaluateExpression({0xc0000c1318, 0x3}, {0xc000072e3f, 0x121, 0x121})
```

```
        /tmp/lima/pkg/yqutil/yqutil.go:47 +0x796
github.com/lima-vm/lima/pkg/yqutil.TestEvaluateExpressionPoc(0xc0000fb860?)
        /tmp/lima/pkg/yqutil/yqutil_test.go:12 +0x86
testing.tRunner(0xc0000fb860, 0x9d0b50)
        /usr/lib/go-1.22/src/testing/testing.go:1689 +0xfb
created by testing.(*T).Run in goroutine 1
        /usr/lib/go-1.22/src/testing/testing.go:1742 +0x390
exit status 2
FAIL    github.com/lima-vm/lima/pkg/yqutil      0.013s
```

Memory exhaustion when evaluating expression

Severity	Low
Status	Reported
id	ADA-LIMA-FUZZ-2024-9
Affected Lima Component	github.com/lima-vm/lima/pkg/yqutil
OSS-Fuzz issue	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=70693

This is a memory exhaustion issue of the entire system that a fuzzer can trigger with a small string passed to `EvaluateExpression`. This can cause denial of service of Lima as well as other services on the machine.

Proof of concept

Lima commit: 6c2bfaa9197b54c8cc5a93707e65e22422b0616c
`lima/pkg/yqutil/yqutil_test.go`

Before running the below unit test, open a tab with `top`. Then run the unit test in another tab.

```go
func TestEvaluateExpressionPoc(t *testing.T) {
        expression := string([]byte{34, 45, 34, 52, 56, 37, 37, 52, 52,
            52, 52, 52, 52, 42, 61, 52, 52, 52, 52, 52, 52, 52, 52, 52,
            52, 42, 61, 52, 52, 42, 61, 52, 52, 52})
        content := []byte{54, 52, 44, 33, 52, 98, 111, 111, 52}
        _, _ = EvaluateExpression(expression, content)
}
```

The memory usage will start to climb and might ultimately result in a denial of service of the machine.

Divide by zero panic

Severity	Low
Status	Reported
id	ADA-LIMA-FUZZ-2024-10
Affected Lima Component	‘github.com/lima-vm/lima/pkg/yqutil‘
OSS-Fuzz issue	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=70775

A fuzzer was able to generate a file that triggered a divide by zero panic in a 3rd-party dependency when passed to `ConvertToRaw`.

Proof of concept

```go
package nativeimgutil

import (
        "os"
        "path/filepath"
        "testing"
)

func TestConvertToRawPoC(t *testing.T) {
        imgData := []byte{81, 70, 73, 251, 49, 56, 18, 0, 0, 0, 0, 0,
            0, 0, 0, 0, 0, 0, 0, 0, 0, 126, 54, 49, 0, 0, 0, 0, 0, 0, 0,
             8, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0,
             0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 236, 0, 0, 0,
            0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 32, 0, 0, 0, 0, 0, 0, 0, 0, 0,
             0, 0, 0, 0, 0, 0, 0, 0, 17, 0, 0, 0, 0, 0, 0}
        withBacking := false
        size := int64(32)
        srcPath := filepath.Join(t.TempDir(), "src.img")
        destPath := filepath.Join(t.TempDir(), "dest.img")
        err := os.WriteFile(srcPath, imgData, 0o600)
        if err != nil {
                return
        }
        _ = ConvertToRaw(srcPath, destPath, &size, withBacking)
}
```

Stacktrace

```
--- FAIL: TestConvertToRawPoC (0.00s)
panic: runtime error: integer divide by zero [recovered]
        panic: runtime error: integer divide by zero

goroutine 19 [running]:
testing.tRunner.func1.2({0x6b22e0, 0x926fb0})
        /usr/lib/go-1.22/src/testing/testing.go:1631 +0x24a
testing.tRunner.func1()
        /usr/lib/go-1.22/src/testing/testing.go:1634 +0x377
panic({0x6b22e0?, 0x926fb0?})
        /usr/lib/go-1.22/src/runtime/panic.go:770 +0x132
github.com/lima-vm/go-qcow2reader/image/qcow2.(*Qcow2).ReadAt(0xc0001b8420, {0xc000380000, 0x8, 0x100000}, 0x0)
        /home/adam/go/pkg/mod/github.com/lima-vm/go-qcow2reader@v0.1.1/image/qcow2/qcow2.go:911 +0x1ea
io.(*SectionReader).Read(0xc000192e70, {0xc000380000?, 0x69d920?, 0x1?})
        /usr/lib/go-1.22/src/io/io.go:516 +0x4f
github.com/cheggaaa/pb/v3.(*Reader).Read(0xc00019a2d0, {0xc000380000?, 0x934fa0?, 0xc00019a2d0?})
        /home/adam/go/pkg/mod/github.com/cheggaaa/pb/v3@v3.1.5/io.go:15 +0x28
github.com/lima-vm/lima/pkg/nativeimgutil.copySparse(0xc0001980e8, {0x75fd60, 0xc00019a2d0}, 0x100000)
        /tmp/lima/pkg/nativeimgutil/nativeimgutil.go:134 +0xbd
github.com/lima-vm/lima/pkg/nativeimgutil.ConvertToRaw({0xc0001d8270, 0x2e}, {0xc0001d8330, 0x2f}, 0xc00002ff08, 0x0)
        /tmp/lima/pkg/nativeimgutil/nativeimgutil.go:79 +0xb05
github.com/lima-vm/lima/pkg/nativeimgutil.TestConvertToRawPoC(0xc0001d0820)
        /tmp/lima/pkg/nativeimgutil/my_test.go:19 +0x22d
testing.tRunner(0xc0001d0820, 0x70d318)
        /usr/lib/go-1.22/src/testing/testing.go:1689 +0xfb
created by testing.(*T).Run in goroutine 1
        /usr/lib/go-1.22/src/testing/testing.go:1742 +0x390
exit status 2
FAIL    github.com/lima-vm/lima/pkg/nativeimgutil       0.016s
```

Length of string controllable by user input in 3rd-party yq library

Severity	Low
Status	Reported
id	ADA-LIMA-FUZZ-2024-11
Affected Lima Component	‘github.com/lima-vm/lima/pkg/yqutil‘
OSS-Fuzz issue	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=70775

Proof of concept

Lima commit: 6c2bfaa9197b54c8cc5a93707e65e22422b0616c
lima/pkg/yqutil/yqutil_test.go

```
func TestEvaluateExpressionPoc(t *testing.T) {
        expression := string([]byte{34, 223, 221, 13, 39, 13, 38, 255,
               216, 254, 223, 217, 216, 221, 221, 221, 221, 34, 45, 50, 46,
                52, 54, 55, 55, 57, 48, 42, 55, 49, 48, 50, 54, 57, 50, 53,
                54, 57, 53, 51, 53, 58})
        content := []byte{}
        _, _ = EvaluateExpression(expression, content)
}
```

Stacktrace

```
--- FAIL: TestEvaluateExpressionPoc (0.00s)
panic: runtime error: makeslice: len out of range [recovered]
        panic: runtime error: makeslice: len out of range

goroutine 6 [running]:
testing.tRunner.func1.2({0x91fd00, 0xa685f0})
        /usr/lib/go-1.22/src/testing/testing.go:1631 +0x24a
testing.tRunner.func1()
        /usr/lib/go-1.22/src/testing/testing.go:1634 +0x377
panic({0x91fd00?, 0xa685f0?})
        /usr/lib/go-1.22/src/runtime/panic.go:770 +0x132
internal/bytealg.MakeNoZero(0x8000000000000000?)
        /usr/lib/go-1.22/src/runtime/slice.go:367 +0x79
strings.(*Builder).grow(0xc0002b6a08, 0xd?)
```

```
	/usr/lib/go-1.22/src/strings/builder.go:69 +0x27
strings.(*Builder).Grow(0xc0002b6a38?, 0x821729?)
	/usr/lib/go-1.22/src/strings/builder.go:83 +0x50
strings.Repeat({0xc00002edc0?, 0x28}, 0xc0002b6aa8?)
	/usr/lib/go-1.22/src/strings/strings.go:580 +0xbc
github.com/mikefarah/yq/v4/pkg/yqlib.repeatString(0x7ac7b1?, 0xc1a49d6dabf1185e?)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_multiply.go:157 +0x94
github.com/mikefarah/yq/v4/pkg/yqlib.multiplyScalars(0xc0002428c0, 0xc0002429a0)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_multiply.go:95 +0x208
github.com/mikefarah/yq/v4/pkg/yqlib.multiplyOperator.multiply.func1(0xeb0180, {0xc000300600, 0xc000300660, 0x0, {0x0, 0x0}}, 0xc0002428c0, 0xc0002429a0)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_multiply.go:76 +0x3e5
github.com/mikefarah/yq/v4/pkg/yqlib.resultsForRHS(0xeb0180, {0xc000300600, 0xc000300660, 0x0, {0x0, 0x0}}, 0xc0002428c0, {0x0, 0x0, 0xc0002b70f8}, ...)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:94 +0x61a
github.com/mikefarah/yq/v4/pkg/yqlib.doCrossFunc(0xeb0180, {0xc000300600, 0xc000300660, 0x0, {0x0, 0x0}}, 0xc000012588, {0x0, 0x0, 0xc0002b70f8})
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:131 +0x408
github.com/mikefarah/yq/v4/pkg/yqlib.crossFunctionWithPrefs(0xeb0180, {0xc000300480, 0xc0003004e0, 0x0, {0x0, 0x0}}, 0xc000012588, {0x0, 0x0, 0xc0002b70f8})
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:164 +0x398
github.com/mikefarah/yq/v4/pkg/yqlib.crossFunction(0xc00010b9e0?, {0xc000300480, 0xc0003004e0, 0x0, {0x0, 0x0}}, 0x0?, 0xc0003081a0?, 0xe0?)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:142 +0x93
github.com/mikefarah/yq/v4/pkg/yqlib.multiplyOperator(0xeb0180, {0xc000300480, 0xc0003004e0, 0x0, {0x0, 0x0}}, 0xc000012588)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_multiply.go:33 +0x158
github.com/mikefarah/yq/v4/pkg/yqlib.(*dataTreeNavigator).GetMatchingNodes(0xeb0180, {0xc000300480, 0xc0003004e0, 0x0, {0x0, 0x0}}, 0xc000012588)
	/home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/data_tree_navigator.go:65 +0x21f
github.com/mikefarah/yq/v4/pkg/yqlib.resultsForRHS(0xeb0180, {0xc000300480, 0xc0003004e0, 0x0, {0x0, 0x0}}, 0xc0002427e0, {0x0, 0x0, 0xc0002b77d8}, ...)
```

```
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:73 +0x210
github.com/mikefarah/yq/v4/pkg/yqlib.doCrossFunc(0xeb0180, {0xc000300480, 0xc0003004e0, 0x0, {0x0, 0x0}}, 0xc0000125a0, {0x0, 0x0, 0xc0002b77d8})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:131 +0x408
github.com/mikefarah/yq/v4/pkg/yqlib.crossFunctionWithPrefs(0xeb0180, {0xc0003003c0, 0xc000300420, 0x0, {0x0, 0x0}}, 0xc0000125a0, {0x0, 0x0, 0xc0002b77d8})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:164 +0x398
github.com/mikefarah/yq/v4/pkg/yqlib.crossFunction(0xc0002b7840?, {0xc0003003c0, 0xc000300420, 0x0, {0x0, 0x0}}, 0x1?, 0x7f87636d4c58?, 0x17?)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operators.go:142 +0x93
github.com/mikefarah/yq/v4/pkg/yqlib.sequenceFor(0xeb0180, {0xc000300330, 0x0, 0x0, {0x0, 0x0}}, 0xc000242700, 0xc0000125a0)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_create_map.go:55 +0x3f3
github.com/mikefarah/yq/v4/pkg/yqlib.createMapOperator(0xeb0180, {0xc000300330, 0x0, 0x0, {0x0, 0x0}}, 0xc0000125a0)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/operator_create_map.go:19 +0x385
github.com/mikefarah/yq/v4/pkg/yqlib.(*dataTreeNavigator).GetMatchingNodes(0xeb0180, {0xc000300330, 0x0, 0x0, {0x0, 0x0}}, 0xc0000125a0)
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/data_tree_navigator.go:65 +0x21f
github.com/mikefarah/yq/v4/pkg/yqlib.(*streamEvaluator).EvaluateNew(0xc0002b7e30, {0xc00002a660?, 0xc0002b7e30?}, {0xa6e328, 0xc0002ea3f0})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/stream_evaluator.go:38 +0x1df
github.com/mikefarah/yq/v4/pkg/yqlib.(*streamEvaluator).EvaluateFiles(0xc0002b7e30, {0xc00002a660, 0x2a}, {0xc0002b7e20, 0x1, 0x0?}, {0xa6e328, 0xc0002ea3f0}, {0xa6b498, 0xc0002ea460})
        /home/adam/go/pkg/mod/github.com/mikefarah/yq/v4@v4.44.2/pkg/yqlib/stream_evaluator.go:72 +0x215
github.com/lima-vm/lima/pkg/yqutil.EvaluateExpression({0xc00002a660, 0x2a}, {0xc000077f60, 0x0, 0x0})
        /tmp/lima/pkg/yqutil/yqutil.go:47 +0x796
github.com/lima-vm/lima/pkg/yqutil.TestEvaluateExpressionPoc(0xc00013f520?)
        /tmp/lima/pkg/yqutil/yqutil_test.go:12 +0x96
testing.tRunner(0xc00013f520, 0x9d0b50)
        /usr/lib/go-1.22/src/testing/testing.go:1689 +0xfb
created by testing.(*T).Run in goroutine 1
        /usr/lib/go-1.22/src/testing/testing.go:1742 +0x390
exit status 2
```

```
FAIL    github.com/lima-vm/lima/pkg/yqutil      0.020s
```