

AIによるOpen Source Routing Protocol実装の
Security Checkとzebra-rsのパフォーマンス測定

ENOG89
Kunihiro Ishiguro

オープンソース成功の代償 CVEへの対応

- FRR

ultrathink. We want to find potential crash issue regarding packet parser. Please take a look into previously found issue in here:

<https://www.cvedetails.com/vendor/17227/Frrouting.html>

And investigate other issue in codes.

- gobgp

ultrathink. Please investigate potential buffer overrun or crash issue

- zebra-rs

ultrathink. Please investigate potential buffer overrun or crash issue in @crates/isis-packet and write down the result into markdown file.

isis-packet Security Audit: Buffer Overrun and Crash Issues

Summary

Found **9 issues** across the crate. The most common patterns are unchecked `split_at()` calls with untrusted TLV lengths, unchecked slice indexing in checksum code, and u8 cast truncation in length calculations.

Critical (CRASH/Panic from malformed packets)

1. Unchecked buffer indexing in checksum validation

- **File:** `src/checksum.rs:2`
- **Code:**

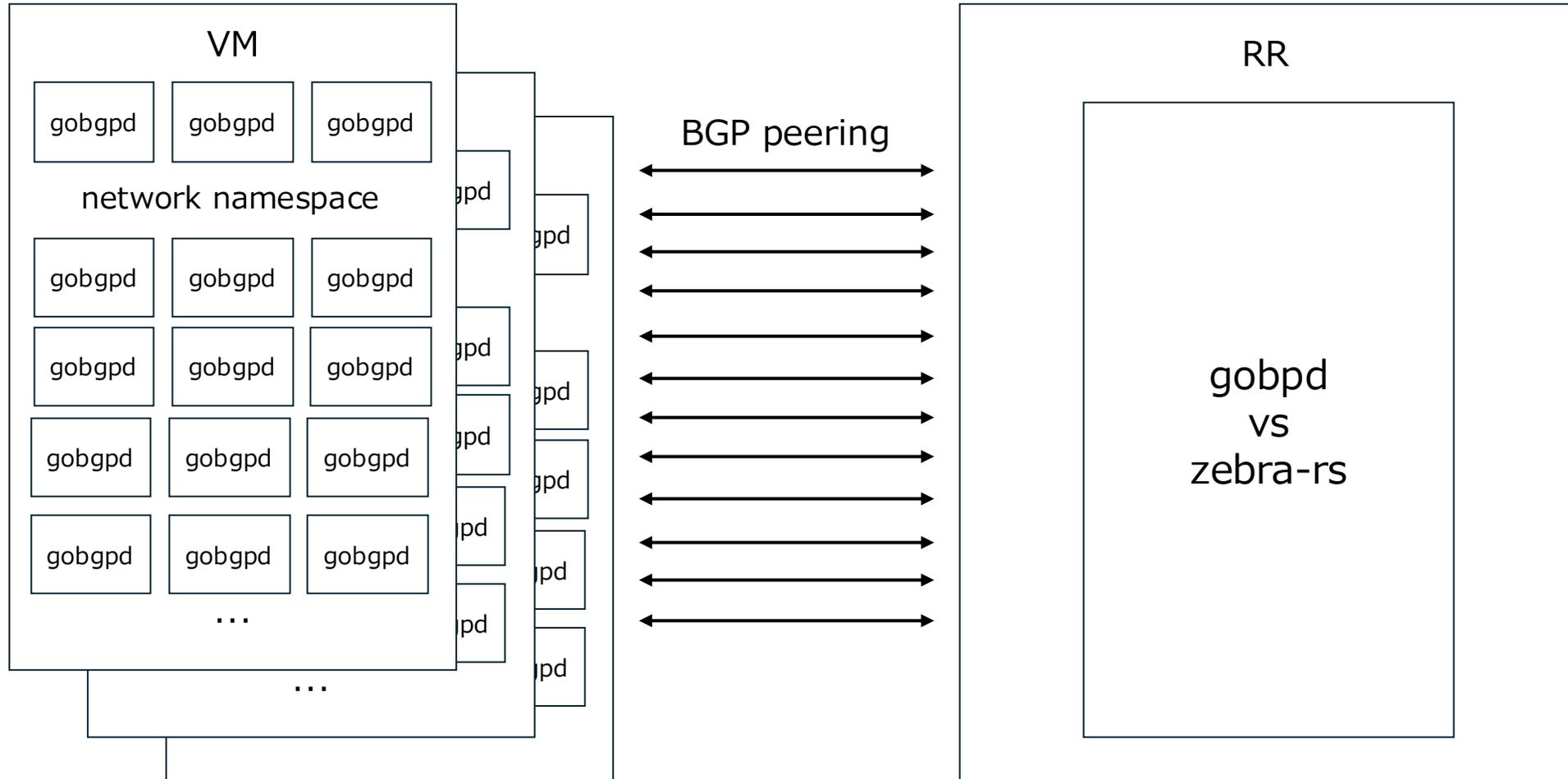
```
pub fn is_valid_checksum(input: &[u8]) -> bool {
    fletcher::calc_fletcher16(&input[12..]) == 0
}
```

- **Problem:** Direct slice index `input[12..]` panics if `input.len() < 12`.
- **Trigger:** Any IS-IS packet smaller than 12 bytes.
- **Fix:** Return `false` if `input.len() < 12`.

2. Unchecked buffer indexing in LSP checksum writing

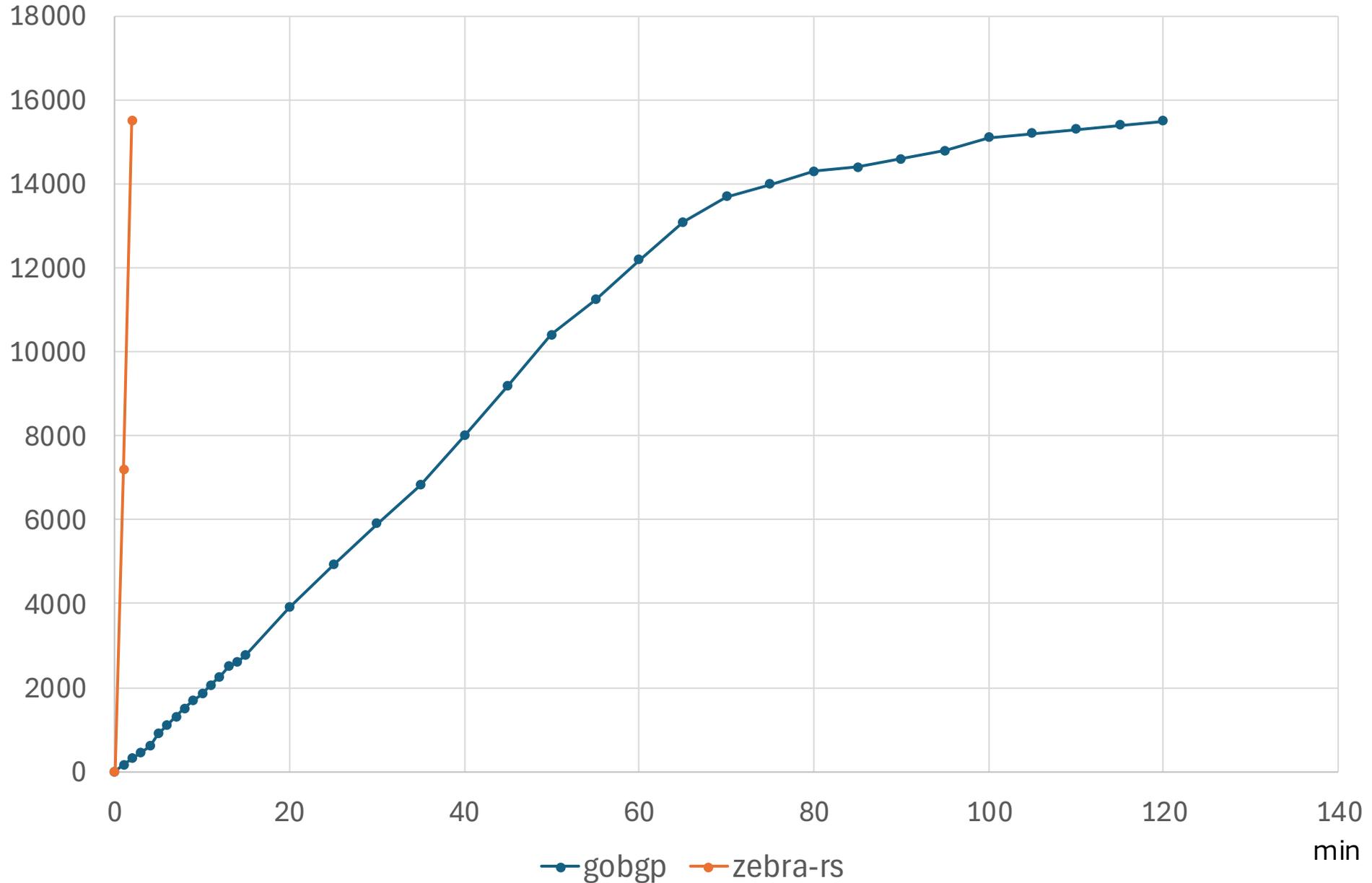
Performance Measurement

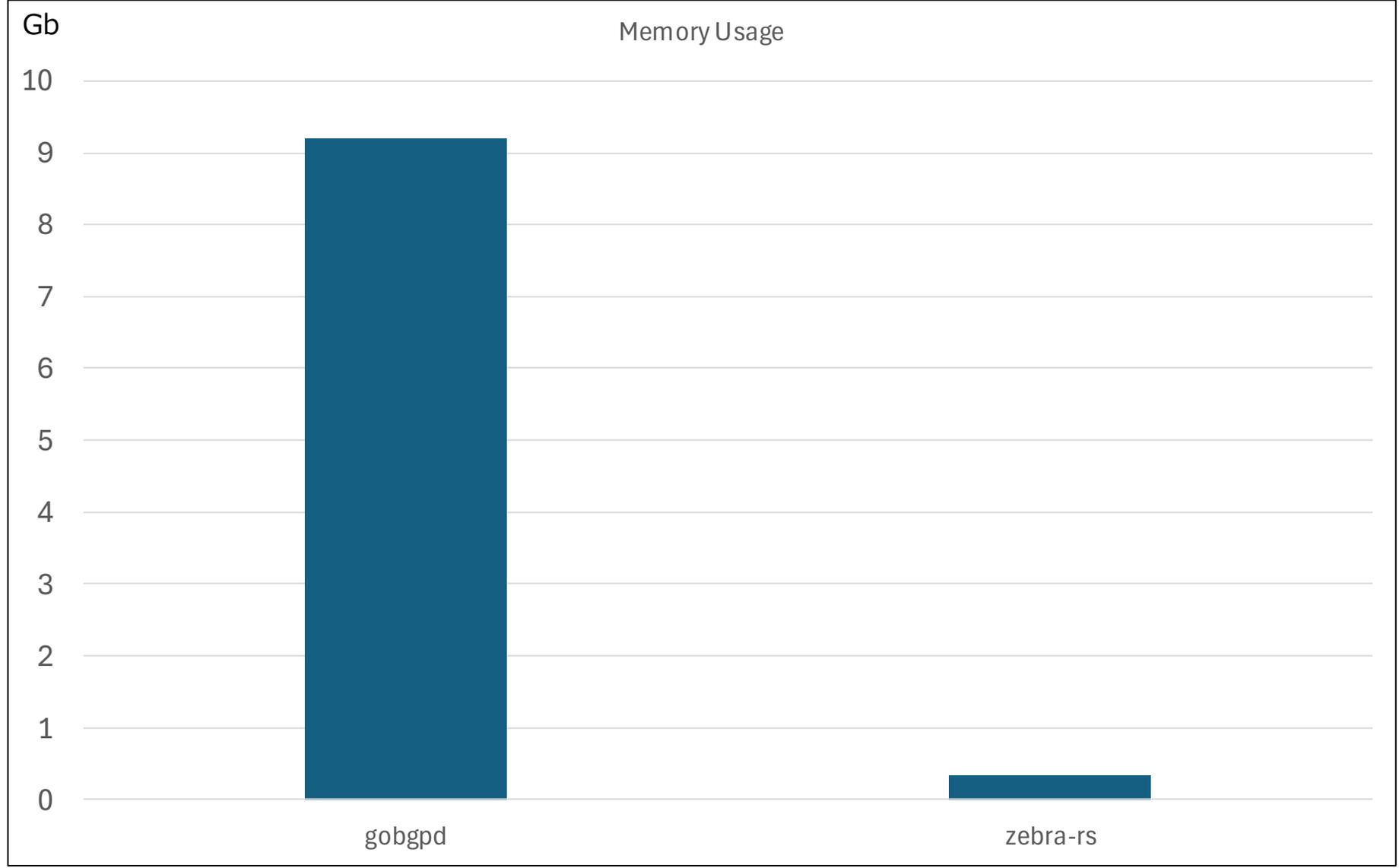
RR1の経路をエミュレート: Peer: 1799, Routes: 15073



Routing Table Convergence (gobgp vs zebra-rs)

No of Routes





Async implementation of BGP

```
connection: http://127.0.0.1:6669/ (CONNECTED)
views: t = tasks, r = resources
controls: select column (sort) = ← or h, l, scroll = ↑↓ or k, j, view details = ↵, invert sort (highest/lowest) = i, scroll to top = gg, scroll to bottom = G, toggle pause = space,
quit = q
```

Warnings

```
△ 1 tasks have been boxed by the runtime due to their size
△ 1 tasks are 1024 bytes or larger
```

Tasks (83) ▶ Running (0) ▮ Idle (15)

Warn	ID	State	Name	Total	Busy	Sched	Idle	Polls	Kind	Location	Fields
	109	▮		1m05s	5ms	837μs	1m04s	9	task	zebra/src/fib/netlink/handle.rs:54:9	size.bytes=320 target=tokio::task
	110	▮		1m05s	78μs	0ns	1m05s	1	task	zebra/src/fib/netlink/handle.rs:57:9	size.bytes=32 target=tokio::task
△ 1	113	▮		40s	594μs	0ns	40s	1	task	zebra/src/config/serve.rs:275:5	size.bytes=2048 target=tokio::task
	114	▮		40s	34ms	2ms	40s	69	task	zebra/src/policy/inst.rs:43:5	size.bytes=272 target=tokio::task
	115	▮		40s	1s	68ms	39s	386	task	zebra/src/bgp/inst.rs:151:5	size.bytes=936 target=tokio::task
△ 1	116	▮		40s	35ms	2ms	40s	48	task	zebra/src/rib/inst.rs:195:5	original_size.bytes=2096 size.bytes=8 target=tokio::task
	117	▮		40s	187μs	0ns	40s	1	task	zebra/src/rib/inst.rs:198:5	size.bytes=144 target=tokio::task
	118	▮		40s	2ms	6ms	40s	16	task	zebra/src/bgp/task.rs:20:26	size.bytes=240 target=tokio::task
	449	▮		39s	17ms	0ns	39s	1	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	461	▮		39s	8ms	0ns	39s	1	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	471	▮		39s	7ms	0ns	39s	1	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	480	▮		39s	5ms	0ns	39s	1	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	506	▮		39s	203μs	0ns	39s	1	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	514	▮		39s	143μs	0ns	39s	1	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	516	▮		39s	151μs	0ns	39s	1	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	570	▮		7s	285μs	666μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	571	▮		7s	217μs	645μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	572	▮		7s	183μs	764μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	574	▮		7s	225μs	514μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	576	▮		7s	314μs	706μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	573	▮		7s	213μs	185μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	575	▮		7s	184μs	468μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	577	▮		7s	209μs	627μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	578	▮		7s	173μs	628μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	579	▮		7s	195μs	840μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	580	▮		7s	287μs	157μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	582	▮		7s	193μs	348μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	584	▮		7s	197μs	461μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	586	▮		7s	324μs	674μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	589	▮		7s	306μs	349μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	588	▮		7s	233μs	1ms	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	587	▮		7s	338μs	356μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	590	▮		7s	183μs	1ms	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	591	▮		7s	208μs	1ms	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	605	▮		7s	307μs	1ms	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	615	▮		7s	330μs	320μs	7s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task
	625	▮		5s	2ms	2ms	5s	4	task	zebra/src/bgp/task.rs:62:9	size.bytes=336 target=tokio::task
	624	▮		5s	2ms	456μs	5s	4	task	zebra/src/bgp/task.rs:62:9	size.bytes=336 target=tokio::task
	613	▮		5s	2ms	482μs	5s	4	task	zebra/src/bgp/task.rs:62:9	size.bytes=336 target=tokio::task
	583	▮		5s	2ms	230μs	5s	4	task	zebra/src/bgp/task.rs:62:9	size.bytes=336 target=tokio::task
	602	▮		5s	2ms	454μs	5s	4	task	zebra/src/bgp/task.rs:62:9	size.bytes=336 target=tokio::task
	607	▮		5s	2ms	119μs	5s	4	task	zebra/src/bgp/task.rs:62:9	size.bytes=336 target=tokio::task
	569	▮		3s	251μs	1ms	3s	3	task	zebra/src/bgp/task.rs:20:26	size.bytes=248 target=tokio::task