What's new in Go

Maksim Terekhin – July 2023

Minor revision

Go 1.20.6 / 1.19.11 – 2023-07-11

- Security fix
  - net/http: insufficient sanitization of Host header (CVE-2023-29406)
- 1.20.6
  - bug fixes to the compiler, `cgo`, the `cover tool`, the `go` command, the runtime, and the `crypto/ecdsa`, `go/build`, `go/printer`, `net/mail`, and `text/template` packages.
- 1.19.11
  - bug fixes to `cgo`, the `cover` tool, the `go` command, the runtime, and the `go/printer` package
- Debian buster docker images are no longer supported (commit)

net/http: insufficient sanitization of Host header

```
+
+ func TestRequestSanitization(t *testing.T) { run(t, testRequestSanitization) }
+ func testRequestSanitization(t *testing.T, mode testMode) {
+         if mode == http2Mode {
+                 // Remove this after updating x/net.
+                 t.Skip("https://go.dev/issue/60374 test fails when run with HTTP/2")
+         }
+         ts := newClientServerTest(t, mode, HandlerFunc(func(rw ResponseWriter, req
  *Request) {
+                 if h, ok := req.Header["X-Evil"]; ok {
+                         t.Errorf("request has X-Evil header: %q", h)
+                 }
+         })).ts
+         req, _ := NewRequest("GET", ts.URL, nil)
+         req.Host = "go.dev\r\nX-Evil:evil"
+         resp, _ := ts.Client().Do(req)
+         if resp != nil {
+                 resp.Body.Close()
+         }
+ }
```

Govulncheck v1.0.0 is released!

- stable API available
- Go Vulnerability Database
- Security best practices guide
- `govulncheck` tutorial

Go Vulnerability Database

Data about new vulnerabilities come directly from Go package maintainers or sources such as MITRE and GitHub. Reports are curated by the Go Security team. Learn more at go.dev/security/vuln.

Search

Search by GO ID, alias, or import path Submit

Recent Reports

GO-2023-1904

CVE-2022-47931 | Affects: github.com/bnb-chain/tss-lib, github.com/binance-chain/tss-lib | Published: Jul 11, 2023

Collision of hash values in github.com/bnb-chain/tss-lib.

Proposals / Discussion

- runtime: change mutex profile to scale contention by number of blocked goroutines (Accepted ✅, scheduled for 1.22)
- proposal: x/net/quic: add QUIC implementation (Likely to accept ⏱️)
- net/http: move HTTP/2 into the standard library (Discussion 💬)
- net/http: add methods and path variables to ServeMux patterns (Discussion 💬)

net/http: add methods and path variables to ServeMux

```
/item/
POST /item/{user}
/item/{user}
/item/{user}/{id}
/item/{$}
POST alt.com/item/{user}
```

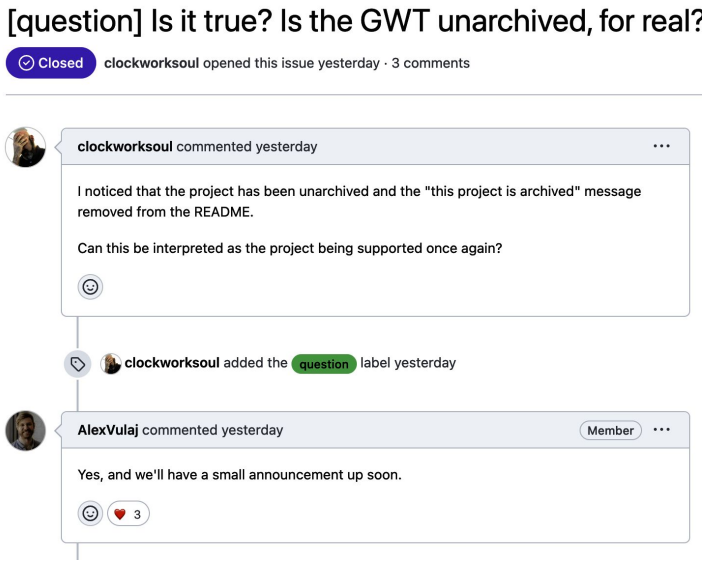
```
package http

func (*Request) PathValue(wildcardName string) string
```

Go 1.21 in August 2023!

- redefining for loop variable semantics: LoopvarExperiment
- The new log/slog package provides structured logging with levels
- Performance improvements for runtime/trace (smaller CPU cost, up to a 10x)

GWT is back 🚀

[Is the GWT unarchived, for real?](#) (PR)



Project Status Update - Jul 17, 2023

We were going to wait until the transition was complete to make an announcement, but it seems that the cat is out of the bag...

We are excited to confirm that the Gorilla web toolkit project has a new group of Core Maintainers!

We are all thrilled by the positive response from the community so far. Here is a list of what we are currently working on to complete the transition process:

- Updating the project to support the latest Go version
- Implementing GitHub features such as Branch Protection, GitHub Actions, and more.
- Updating documentation for contributing, code of conduct, reporting vulnerabilities, etc.

Questions?