fix: replace http.DefaultServeMux fallback with safe defaults #3814

Open Yanhu007 wants to merge 1 commit into `go-kratos:main` from `Yanhu007:fix/remove-default-serve…`

Yanhu007 commented 2 weeks ago

Fixes #3810

Security Issue

The HTTP server sets `http.DefaultServeMux` as the fallback handler for unmatched routes and disallowed methods. Since `DefaultServeMux` is a global shared instance, packages that register handlers in `init()` (most notably `net/http/pprof`) are inadvertently exposed to the network.

Any request to an unregistered route (e.g. `/debug/pprof/`) falls through to `DefaultServeMux`, potentially exposing profiling data, goroutine dumps, and heap profiles.

Fix

Replace with safe defaults:

- `http.NotFoundHandler()` for `NotFoundHandler` (returns 404)
- A simple 405 handler for `MethodNotAllowedHandler`

Users who need the previous behavior can explicitly opt-in using the existing `NotFoundHandler()` and `MethodNotAllowedHandler()` server options added in #3131.

Breaking Change

This is technically a breaking change for anyone relying on the `DefaultServeMux` fallback behavior, but the previous default was a security risk. The `NotFoundHandler()` and `MethodNotAllowedHandler()` options provide a migration path.

 `fix: replace http.DefaultServeMux fallback handlers with safe defaults` ··· ✓ `0284a5b`

dosubot Bot added the size:XS label 2 weeks ago

Reviewers

No reviews

Assignees

No one assigned

Labels

size:XS

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

Unintended Route Exposure via DefaultServeMux Fallback

1 participant