golang / go Public

<> Code ⊙ Issues 5k+ Pull requests 302 Discussions Actions ···

New issue

Jump to bottom

net/http: improper sanitization of Transfer-Encoding header #53188

Closed **neild** opened this issue on Jun 1 · 6 comments

Labels	NeedsFix release-blocker Security
Milestone	Go1.19

neild commented on Jun 1 Contributor

The `net/http` server improperly strips CRs surrounding the `Transfer-Encoding` header value, treating `"Transfer-Encoding: \rchunked"` as indicating a chunked body.

For example, this request is interpreted as containing the body `a`.

```
echo -ne "POST /post HTTP/1.1\r\nHost: localhost\r\nTransfer-Encoding:
\rchunked\r\n\r\n1\r\na\r\n0\r\n\r\n" | nc localhost 8080
```

This is a weak vector for request smuggling: CRs are not permitted in headers aside from in the CRLF line terminators, so this request is invalid. We should still fix this as a general hardening measure.

Thanks to Zeyu Zhang (https://www.zeyu2001.com/) for reporting this issue.

gopherbot commented on Jun 1

Change https://go.dev/cl/409874 mentions this issue: `net/http: don't strip whitespace from Transfer-Encoding headers`

dmitshur added the **NeedsFix** label on Jun 3

dmitshur added this to the **Go1.19** milestone on Jun 3

gopherbot commented on Jun 6

Change https://go.dev/cl/410714 mentions this issue: `net/textproto: reject invalid header keys/values in ReadMIMEHeader`

neild commented on Jun 17 Contributor Author

@gopherbot please open backport issues.

gopherbot mentioned this issue on Jun 17

net/http: improper sanitization of Transfer-Encoding header [1.17 backport] #53432

Closed

gopherbot commented on Jun 17

Backport issue(s) opened: #53432 (for 1.17), #53433 (for 1.18).

Remember to create the cherry-pick CL(s) as soon as the patch is submitted to master, according to https://go.dev/wiki/MinorReleases.

gopherbot mentioned this issue on Jun 17

net/http: improper sanitization of Transfer-Encoding header [1.18 backport] #53433

Closed

gopherbot closed this as completed in `e5017a9` on Jun 29

gopherbot commented on Jun 29

Change https://go.dev/cl/415217 mentions this issue: `[release-branch.go1.17] net/http: don't strip whitespace from Transfer-Encoding headers`

gopherbot commented on Jun 29

Change https://go.dev/cl/415218 mentions this issue: `[release-branch.go1.18] net/http: don't strip whitespace from Transfer-Encoding headers` tatianab added Security release-blocker labels on Jun 29

gopherbot pushed a commit that referenced this issue on Jul 12

`[release-branch.go1.17] net/http: don't strip whitespace from Transfe…` … d13431c

gopherbot pushed a commit that referenced this issue on Jul 12

`[release-branch.go1.18] net/http: don't strip whitespace from Transfe…` … 222ee24

bradfitz pushed a commit to tailscale/go that referenced this issue on Jul 13

`[release-branch.go1.18] net/http: don't strip whitespace from Transfe…` … 61d05bd

tatianab mentioned this issue on Jul 14

x/vulndb: potential Go vuln in std: CVE-2022-1705 golang/vulndb#525

Closed

jproberts pushed a commit to jproberts/go that referenced this issue on Aug 9

`net/http: don't strip whitespace from Transfer-Encoding headers` … 2ded4a8

danbudris pushed a commit to danbudris/go that referenced this issue on Sep 9

`[release-branch.go1.17] net/http: don't strip whitespace from Transfe…` … d51c433

danbudris pushed a commit to danbudris/go that referenced this issue on Sep 9

`[release-branch.go1.17] net/http: don't strip whitespace from Transfe…` … 36ad18d

danbudris pushed a commit to danbudris/go that referenced this issue on Sep 12

`[release-branch.go1.17] net/http: don't strip whitespace from Transfe…` … 6ede48b

danbudris pushed a commit to danbudris/go that referenced this issue on Sep 14

`[release-branch.go1.17] net/http: don't strip whitespace from Transfe…` … b8c48c1

rcrozean pushed a commit to rcrozean/go that referenced this issue on Oct 5

`net/http: don't strip whitespace from Transfer-Encoding headers` … c3c7086

rcrozean pushed a commit to rcrozean/go that referenced this issue on Oct 12

`net/http: don't strip whitespace from Transfer-Encoding headers` … 895d987

rcrozean pushed a commit to rcrozean/go that referenced this issue on Oct 12

`net/http: don't strip whitespace from Transfer-Encoding headers` … 891dd82

gopherbot pushed a commit that referenced this issue 18 days ago

`net/textproto: reject invalid header keys/values in ReadMIMEHeader` … a6642e6

Assignees

No one assigned

Labels

NeedsFix release-blocker Security

Projects

Release Status & Blockers (1.20)

Status: Done

+1 more

Milestone

Go1.19

Development

No branches or pull requests

4 participants