Security Considerations for Optimistic Protocol Transitions in HTTP/1.1

Ben Schwartz, Meta Platforms, Inc.

HTTPBIS @ IETF 122

Unsafe HTTP CONNECT is a real thing

- I searched Github for `CONNECT.*HTTP\/1.1` in Python code
- First 50 results included at least 4 distinct clients that assumed success without checking the status code.
  - But still waited for the response!

Changes in -07 - only in “Guidance for HTTP CONNECT”

- #2944 Clearly limit recommendations to HTTP/1.1
- #2997 Adjust text related to HTTP/1.1 CONNECT

In HTTP/1.1, proxy clients that send CONNECT requests on behalf of untrusted TCP clients MUST wait for a 2xx (Successful) response before forwarding any TCP payload data. Proxy clients that start forwarding before confirming the response status code are vulnerable to a trivial request smuggling attack (Section 3.1).

To mitigate the impact of such vulnerable clients, proxy servers MAY close the underlying connection when rejecting an HTTP/1.1 CONNECT request, without processing any further data on that connection. Note that this behavior will frequently impair the performance of correctly implemented clients, especially when returning a "407 (Proxy Authentication Required)" response. This performance loss can be be avoided by using HTTP/2 or HTTP/3, which are not vulnerable to this attack.

Open Issue #2739 - What to tell the server?

Current text: *To mitigate the impact of such vulnerable clients, proxy servers MAY close the underlying connection when rejecting an HTTP/1.1 CONNECT request*

Should we change “MAY” to “MUST” or “SHOULD”?

- Recommendation based on knowledge of the deployment scenario?
- User-Agent sniffing to identify safe/vulnerable clients?

A change to “MUST” would presumably require Updating RFC 9112.

(Also, what about Upgrade?)

WGLC!

0\r\n
\r\n