Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 22, 2014

M. Nottingham

June 20, 2014

The Over-Version HTTP Response Header Field
draft-nottingham-http-over-version-00

Abstract

The 505 (HTTP Version Not Supported) status code does not clearly indicate, on its own, the scope of the assertion, nor the version(s) supported. This document introduces a new header field, "Over-Version", to indicate this information.

Table of Contents

1. Introduction

The semantics of the 505 (Version Not Supported) status code are defined by [RFC7231] as:

The 505 (HTTP Version Not Supported) status code indicates that the server does not support, or refuses to support, the major version of HTTP that was used in the request message. The server is indicating that it is unable or unwilling to complete the request using the same major version as the client, as described in Section 2.6 of [RFC7230], other than with this error message. The server should generate a representation for the 505 response that describes why that version is not supported and what other protocols are supported by that server.

This document defines a new HTTP response header, "Over-Version", to be used in 505 responses to specify the protocol version(s) that can be used, what resource(s) that assertion applies to, and how long it is valid for (leveraging Cache-Control).

1.1. Use Case: TLS Client Authentication

While Over-Version might have a variety of applications, the primary use case for them is the signaling that a resource (or set of resources) requires TLS Client Authentication in HTTP/2 [I-D.ietf-httpbis-http2]. Since TLS renegotiation has been forbidden in that protocol, a means of signaling that a particular request should be made on a HTTP/1.1 connection is needed, so that a client can use that protocol, allowing the server to perform renegotiation to initiate client authentication.

1.2. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Furthermore, this document uses the Augmented BNF defined in [RFC5234], along with the #rule list extension defined in [RFC7230], Section 7.

2. The Over-Version HTTP Header Field

The Over-Version HTTP Header field, when occurring in 505 (Version Not Supported) responses, asserts the version or versions of HTTP that are supported, and what resource(s) the assertion applies to, and optionally how long it lasts.

Over-Version = 1*(OWS ";" OWS parameter)

This document specifies the following over-version parameters:

- "scope" - one of "origin", "resource" or "prefix" (see below)

- "version-id" - a space-separated list of ALPN protocol identifiers [I-D.ietf-tls-applayerprotoneg].

Additionally, when Over-Version is in use, it indicates that the Cache-Control header conveys a cache policy that is applicable to this information (as well as the response itself).

For example:

```
HTTP/1.1 505 Version Not Supported
Over-Version: scope="prefix", version-id="h2"
Cache-Control: max=age=60
```

This response indicates that the requested resource and its children cannot be reached over the current protocol version, and that for the next 60 seconds, the client can successfully request them using the "h2" protocol (in this case, HTTP/2).

2.1. Over-Version Scopes

This document defines the following values for the "scope" parameter;

- "origin" - indicates that the over-version applies to all resources on the origin of the request

- "resource" - indicates that the over-version applies to the requested resource only (i.e., matching origin, path, and query)

- "prefix" - indicates that the over-version applies to resources when the origin matches and the requested resource's path segments are a prefix. For example, if the requested resource's path is "/foo" then "/foo", "/foo?bar", "/foo/bar", "/foo/bar/baz" would share the over-version, while "/bar", "/foobar" and "/bar/foo" would not.

3. IANA Considerations

This document registers a new HTTP header field, "Over-Version", into the Permanent Message Header Field Name Registry.

- Header Field Name: Over-Version

- Protocol: HTTP

- Status: standard

- Reference: [this document]

4. Security Considerations

Over-Version can be used to effect a downgrade attack by a man-in-the-middle. When received over an insecure channel, it SHOULD be ignored.

Over-Version can also be used to effect a downgrade attack by a party that has the ability to inject response headers on the same origin. The "origin" scope in particular is able to be misused, and SHOULD be ignored unless the security properties of the new protocol are equal to or better than the existing one.

5. References

5.1. Normative References

[I-D.ietf-tls-applayerprotoneg]
Friedl, S., Popov, A., Langley, A., and S. Emile, "Transport Layer Security (TLS) Application Layer Protocol Negotiation Extension", draft-ietf-tls-applayerprotoneg-05 (work in progress), March 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC7230] Fielding, R. and J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, June 2014.

[RFC7231] Fielding, R. and J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, June 2014.

5.2. Informative References

[I-D.ietf-httpbis-http2]
Belshe, M., Peon, R., and M. Thomson, "Hypertext Transfer Protocol version 2", draft-ietf-httpbis-http2-13 (work in progress), June 2014.

Author's Address

Mark Nottingham

Email: mnot@mnot.net
URI: http://www.mnot.net/