HTTPBIS Working Group
Internet-Draft
Updates: 9113 (if approved)
Intended status: Standards Track
Expires: 24 November 2026

E. Gudzenko
Individual Contributor

23 May 2026

Cipher Suite Selection for HTTP/2 Negotiation over TLS 1.2
draft-gudzenko-httpbis-h2-cipher-selection-00

Abstract

Section 9.2.2 of RFC 9113 identifies, but does not normatively resolve, a failure mode in which the application protocol and the cipher suite are selected independently, resulting in a successfully completed TLS handshake whose negotiated parameters may be rejected at the HTTP/2 layer with an INADEQUATE_SECURITY connection error. This document addresses that gap by adding a SHOULD-level procedure that coordinates cipher suite selection with ALPN negotiation, and updates RFC9113.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 24 November 2026.

Copyright Notice

Table of Contents

1. Introduction

An interoperability hazard between TLS cipher suite selection and Application-Layer Protocol Negotiation (ALPN) [RFC7301] for HTTP/2 [RFC9113] over TLS 1.2 [RFC5246] was raised in [ISSUE-612] during the drafting of [RFC7540], the predecessor of [RFC9113]. The HTTP Working Group's resolution, merged via [PR-644], introduced the list of prohibited cipher suites now codified in Appendix A of [RFC9113], together with the mandatory cipher suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as a guaranteed-available alternative.

This resolution ensures a guaranteed-available h2-compatible cipher suite, but leaves server behavior unspecified when both prohibited and h2-compatible cipher suites are available for negotiation. Section 9.2.2 of [RFC9113] notes the resulting failure mode:

> Note that clients might advertise support of cipher suites that are prohibited in order to allow for connection to servers that do not support HTTP/2. This allows servers to select HTTP/1.1 with a cipher suite that is prohibited in HTTP/2. However, this can result in HTTP/2 being negotiated with a prohibited cipher suite if the application protocol and cipher suite are independently selected.

When a client chooses to enforce the cipher suite requirements of Section 9.2.2 of [RFC9113], it may signal this by tearing down the HTTP/2 connection via GOAWAY with error code INADEQUATE_SECURITY (Section 7 of [RFC9113]). However, Section 9.2.2 of [RFC9113] only acknowledges this failure without prescribing a solution, leaving a preventable failure mode unaddressed.

TLS 1.2 remains widely deployed, and this failure mode affects any TLS 1.2 server where prohibited cipher suites are available alongside h2-compatible cipher suites.

This document adds a SHOULD-level procedure for coordinating cipher suite selection with ALPN negotiation. It does not modify the prohibited cipher suite list in Appendix A of [RFC9113] or the mandatory cipher suite requirement of Section 9.2.2 of [RFC9113]. Instead, it closes the normative gap left open by Section 9.2.2 of [RFC9113], which identifies independent selection as a failure mode but does not prescribe how to prevent it when prevention is possible.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The term "ClientHello" is used as defined in Section 7.4.1.2 of [RFC5246].

The term "h2-compatible cipher suite" refers to any TLS 1.2 cipher suite that is not listed in Appendix A of [RFC9113].

3. Applicability

This document applies to TLS 1.2 [RFC5246] servers that negotiate ALPN [RFC7301] and support HTTP/2 [RFC9113].

This document does not apply to TLS 1.3 [RFC8446]. HTTP/2 over TLS 1.3 is addressed by Section 9.2.3 of [RFC9113].

The procedure specified in Section 4 is most directly relevant to deployments where prohibited cipher suites are present in the negotiation alongside h2-compatible cipher suites.

4. Cipher Suite Selection Procedure

When a TLS 1.2 server receives a ClientHello that includes "h2" in the ALPN extension [RFC7301], and the intersection of cipher suites offered in the ClientHello and supported by the server includes at least one h2-compatible cipher suite, the server SHOULD select an h2-compatible cipher suite.

5. Security Considerations

This document does not modify the cipher suite requirements of Section 9.2.2 of [RFC9113] or the list of prohibited cipher suites in Appendix A of [RFC9113]. The TLS threat model is unchanged. This procedure addresses an availability concern: it prevents connection failures that occur when a prohibited cipher suite is selected despite an h2-compatible one being available for negotiation.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/rfc/rfc5246>.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <https://www.rfc-editor.org/rfc/rfc7301>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9113] Thomson, M., Ed. and C. Benfield, Ed., "HTTP/2", RFC 9113, DOI 10.17487/RFC9113, June 2022, <https://www.rfc-editor.org/rfc/rfc9113>.

7.2. Informative References

[ISSUE-612] HTTP Working Group, "TLS Requirements (Issue #612)", 2014, <https://github.com/httpwg/http2-spec/issues/612>.

[PR-644] HTTP Working Group, "Resolve issue #612 by adding cipher block list", 2014, <https://github.com/httpwg/http2-spec/pull/644>.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <https://www.rfc-editor.org/rfc/rfc7540>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

Acknowledgments

This document was informed by the discussion in [ISSUE-612] and [PR-644] of the httpwg/http2-spec repository, in particular the observation by Sam Hartman at IETF 91 that led to the cipher block list now codified in Appendix A of [RFC9113].

Author’s Address

Egor Gudzenko
Individual Contributor
Moscow
Russian Federation
Email: egor@egl.sh