Stream:	Internet Engineering Task Force (IETF)
RFC:	9916
Updates:	8253
Category:	Standards Track
Published:	January 2026
ISSN:	2070-1721
Authors:	D. Dhody	S. Turner	R. Housley
---	---	---	---
	Huawei	*sn3rd*	*Vigil Security*

RFC 9916
Updates to the Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)

Abstract

Section 3.4 of RFC 8253 specifies TLS connection establishment restrictions for PCEPS; PCEPS refers to usage of TLS to provide a secure transport for the Path Computation Element Communication Protocol (PCEP). This document adds restrictions to specify what PCEPS implementations do if they support more than one version of the TLS protocol and to restrict the use of TLS 1.3's early data.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9916.

Copyright Notice

Table of Contents

1. Introduction 2
2. Conventions 2
3. TLS Connection Establishment Restrictions 3
4. Security Considerations 3
5. IANA Considerations 3
6. References 3
6.1. Normative References 3
6.2. Informative References 4
Acknowledgments 4
Authors' Addresses 4

1. Introduction

Section 3.4 of [RFC8253] specifies TLS connection establishment restrictions for PCEPS; PCEPS refers to usage of TLS to provide a secure transport for the Path Computation Element Communication Protocol (PCEP) [RFC5440]. This document adds restrictions to specify what PCEPS implementations do if they support more than one version of the TLS protocol, e.g., TLS 1.2 [RFC5246] and TLS 1.3 [RFC9846], and to restrict the use of TLS 1.3's early data, which is also known as 0-RTT data. All other provisions set forth in [RFC8253] are unchanged, including connection initiation, message framing, connection closure, certificate validation, peer identity, and failure handling.

2. Conventions

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.

3. TLS Connection Establishment Restrictions

Step 1 in Section 3.4 of [RFC8253] includes restrictions on PCEPS TLS connection establishment. This document adds the following restrictions:

- Implementations that support multiple versions of the TLS protocol **MUST** prefer to negotiate the latest version of the TLS protocol; see Section 4.2.1 of [RFC9846].
- PCEPS implementations that support TLS 1.3 or later **MUST NOT** use early data.

> NOTE: Early data (aka 0-RTT data) is a mechanism defined in TLS 1.3 [RFC9846] that allows a client to send data ("early data") as part of the first flight of messages to a server. Note that TLS 1.3 can be used without early data as per Appendix F.5 of [RFC9846]. In fact, early data is permitted by TLS 1.3 only when the client and server share a Pre-Shared Key (PSK), either obtained externally or via a previous handshake. The client uses the PSK to authenticate the server and to encrypt the early data.

> NOTE: As noted in Section 2.3 of [RFC9846], the security properties for early data are weaker than those for subsequent TLS-protected data. In particular, early data is not forward secret, and there is no protection against the replay of early data between connections. Appendix E.5 of [RFC9846] requires applications not use early data without a profile that defines its use.

4. Security Considerations

The security considerations of PCEP [RFC5440] [RFC8231] [RFC8253] [RFC8281] [RFC8283], TLS 1.2 [RFC5246], TLS 1.3 [RFC9846], and TLS/DTLS recommendations [RFC9325] apply here as well.

5. IANA Considerations

This document has no IANA actions.

6. References

6.1. 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/info/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/info/rfc5246>.

[RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, DOI 10.17487/RFC5440, March 2009, <https://www.rfc-editor.org/info/rfc5440>.

[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/info/rfc8174>.

[RFC8253] Lopez, D., Gonzalez de Dios, O., Wu, Q., and D. Dhody, "PCEPS: Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)", RFC 8253, DOI 10.17487/RFC8253, October 2017, <https://www.rfc-editor.org/info/rfc8253>.

[RFC9325] Sheffer, Y., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 9325, DOI 10.17487/RFC9325, November 2022, <https://www.rfc-editor.org/info/rfc9325>.

[RFC9846] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 9846, DOI 10.17487/RFC9846, January 2026, <https://www.rfc-editor.org/info/rfc9846>.

6.2. Informative References

[RFC8231] Crabbe, E., Minei, I., Medved, J., and R. Varga, "Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE", RFC 8231, DOI 10.17487/RFC8231, September 2017, <https://www.rfc-editor.org/info/rfc8231>.

[RFC8281] Crabbe, E., Minei, I., Sivabalan, S., and R. Varga, "Path Computation Element Communication Protocol (PCEP) Extensions for PCE-Initiated LSP Setup in a Stateful PCE Model", RFC 8281, DOI 10.17487/RFC8281, December 2017, <https://www.rfc-editor.org/info/rfc8281>.

[RFC8283] Farrel, A., Ed., Zhao, Q., Ed., Li, Z., and C. Zhou, "An Architecture for Use of PCE and the PCE Communication Protocol (PCEP) in a Network with Central Control", RFC 8283, DOI 10.17487/RFC8283, December 2017, <https://www.rfc-editor.org/info/rfc8283>.

Acknowledgments

We would like to thank Adrian Farrel, Stephane Litkowski, Cheng Li, and Andrew Stone for their review.

Authors' Addresses

Dhruv Dhody
Huawei
Email: dhruv.ietf@gmail.com

Sean Turner
sn3rd
Email: sean@sn3rd.com

Russ Housley
Vigil Security, LLC
516 Dranesville Road
Herndon, VA 20170
United States of America
Email: housley@vigilsec.com