

Path Computation Element
Internet-Draft
Updates: 8253 (if approved)
Intended status: Standards Track
Expires: 12 July 2024

D. Dhody
Huawei
S. Turner
sn3rd
R. Housley
Vigil Security
9 January 2024

Updates for PCEPS: TLS Connection Establishment Restrictions
draft-ietf-pce-pceps-tls13-04

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 PCEP (Path Computation Element Communication Protocol). 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.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at
<https://datatracker.ietf.org/doc/draft-ietf-pce-pceps-tls13/>.

Discussion of this document takes place on the Path Computation Element Working Group mailing list (<mailto:pce@ietf.org>), which is archived at <https://mailarchive.ietf.org/arch/browse/pce/>. Subscribe at <https://www.ietf.org/mailman/listinfo/pce/>.

Source for this draft and an issue tracker can be found at
<https://github.com/ietf-wg-pce/draft-ietf-pce-pceps-tls13>.

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 12 July 2024.

Copyright Notice

Copyright (c) 2024 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
2. Conventions and Definitions	3
3. TLS Connection Establishment Restrictions	3
4. Security Considerations	3
5. IANA Considerations	4
6. Implementation Status	4
7. References	4
7.1. Normative References	4
7.2. Informative References	5
Acknowledgments	6
Authors' Addresses	6

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 PCEP (Path Computation Element Communication Protocol) [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 [I-D.ietf-tls-rfc8446bis], 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 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.

3. TLS Connection Establishment Restrictions

Section 3.4 of [RFC8253] Step 1 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 [I-D.ietf-tls-rfc8446bis].
- * 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 [I-D.ietf-tls-rfc8446bis] 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 [I-D.ietf-tls-rfc8446bis]. 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 [I-D.ietf-tls-rfc8446bis], 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 [I-D.ietf-tls-rfc8446bis] 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], and [RFC8283]; TLS 1.2 [RFC5246]; TLS 1.3 [I-D.ietf-tls-rfc8446bis], and; [RFC9325] apply here as well.

5. IANA Considerations

There are no IANA considerations.

6. Implementation Status

| Note to the RFC Editor - remove this section before
| publication, as well as remove the reference to RFC 7942.

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC7942]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalogue of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [RFC7942], "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

At the time of posting the -04 version of this document, there are no known implementations of this mechanism. It is believed that one vendor has implementation, but these plans are too vague to make any further assertions.

7. References

7.1. Normative References

[I-D.ietf-tls-rfc8446bis]

Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8446bis-09, 7 July 2023, <<https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8446bis-09>>.

- [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>>.
- [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/rfc/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/rfc/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/rfc/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/rfc/rfc9325>>.

7.2. Informative References

- [RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <<https://www.rfc-editor.org/rfc/rfc7942>>.
- [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/rfc/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/rfc/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/rfc/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