Use of TLS for Email Submission and Access
draft-ietf-uta-tls-for-email-01

Abstract

   This specification updates current recommendation for the use of
   Transport Layer Security (TLS) protocol to provide confidentiality of
   email between a Mail User Agent (MUA) and a Mail Submission Server or
   Mail Access Server. This document updates RFC8314.

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 September 8, 2019.

Table of Contents

1. Introduction

   [RFC8314] defines the minimum recommended version for TLS as version
   1.1. Due to the deprecation of TLS 1.1 in
   [I-D.ietf-tls-oldversions-deprecate], this recommendation is no
   longer valid. Therefore this document updates [RFC8314] so that the
   minimum version for TLS is TLS 1.2.

2. Conventions Used in This Document

   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] when they
   appear in ALL CAPS. These words may also appear in this document in
   lower case as plain English words, absent their normative meanings.

3. Updates to RFC8314

   OLD:

   "4.1. Deprecation of Services Using Cleartext and TLS Versions Less
   Than 1.1"

   NEW:

   "4.1. Deprecation of Services Using Cleartext and TLS Versions Less
   Than 1.2"

   OLD

   "As soon as practicable, MSPs currently supporting Secure Sockets
   Layer (SSL) 2.x, SSL 3.0, or TLS 1.0 SHOULD transition their users to
   TLS 1.1 or later and discontinue support for those earlier versions
   of SSL and TLS."

NEW:

"As soon as practicable, MSPs currently supporting Secure Sockets
Layer (SSL) 2.x, SSL 3.0, TLS 1.0 or TLS 1.1 SHOULD transition their
users to TLS 1.2 or later and discontinue support for those earlier
versions of SSL and TLS."

OLD:

In [Section 4.1](#), the text should be revised from: "It is RECOMMENDED
that new users be required to use TLS version 1.1 or greater from the
start. However, an MSP may find it necessary to make exceptions to
accommodate some legacy systems that support only earlier versions of
TLS or only cleartext."

NEW:

"It is RECOMMENDED that new users be required to use TLS version 1.2
or greater from the start. However, an MSP may find it necessary to
make exceptions to accommodate some legacy systems that support only
earlier versions of TLS or only cleartext."

OLD:

" If, however, an MUA provides such an indication, it MUST NOT
indicate confidentiality for any connection that does not at least
use TLS 1.1 with certificate verification and also meet the minimum
confidentiality requirements associated with that account. "

NEW:

" If, however, an MUA provides such an indication, it MUST NOT
indicate confidentiality for any connection that does not at least
use TLS 1.2 with certificate verification and also meet the minimum
confidentiality requirements associated with that account. "

OLD

" MUAs MUST implement TLS 1.2 [RFC5246] or later. Earlier TLS and
SSL versions MAY also be supported, so long as the MUA requires at
least TLS 1.1 [RFC4346] when accessing accounts that are configured
to impose minimum confidentiality requirements. "

NEW:

" MUAs MUST implement TLS 1.2 [RFC5246] or later e.g TLS 1.3
[RFC8446]. Earlier TLS and SSL versions MAY also be supported, so
long as the MUA requires at least TLS 1.2 [RFC5246] when accessing

accounts that are configured to impose minimum confidentiality
requirements. "

OLD:

" The default minimum expected level of confidentiality for all new
accounts MUST require successful validation of the server's
certificate and SHOULD require negotiation of TLS version 1.2 or
greater. (Future revisions to this specification may raise these
requirements or impose additional requirements to address newly
discovered weaknesses in protocols or cryptographic algorithms. "

NEW:

" The default minimum expected level of confidentiality for all new
accounts MUST require successful validation of the server's
certificate and SHOULD require negotiation of TLS version 1.2 or
greater. (Future revisions to this specification may raise these
requirements or impose additional requirements to address newly
discovered weaknesses in protocols or cryptographic algorithms. "

4. IANA Considerations

None of the proposed measures have an impact on IANA.

5. Security Considerations

The purpose of this document is to document updated recommendations
for using TLS with Email services. Those recommendations are based
on [I-D.ietf-tls-oldversions-deprecate].

6. Acknowledgement

The authors would like to thank Vittorio Bertola for his feedback.

7. References

7.1. Informative References

[RFC4346]   Dierks, T. and E. Rescorla, "The Transport Layer Security
            (TLS) Protocol Version 1.1", RFC 4346,
            DOI 10.17487/RFC4346, April 2006,
            <https://www.rfc-editor.org/info/rfc4346>.

7.2. Normative References

[I-D.ietf-tls-oldversions-deprecate]
          Moriarty, K. and S. Farrell, "Deprecating TLSv1.0 and
          TLSv1.1", draft-ietf-tls-oldversions-deprecate-01 (work in
          progress), November 2018.

[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>.

[RFC8314] Moore, K. and C. Newman, "Cleartext Considered Obsolete:
          Use of Transport Layer Security (TLS) for Email Submission
          and Access", RFC 8314, DOI 10.17487/RFC8314, January 2018,
          <https://www.rfc-editor.org/info/rfc8314>.

[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/info/rfc8446>.

Authors' Addresses

   Loganaden Velvindron
   cyberstorm.mu
   88 Avenue De Plevitz Roches Brunes
   Rose Hill 71259
   Mauritius

   Phone: +230 59762817
   Email: loganaden@gmail.com

   Stephen Farrell
   Trinity College Dublin
   Dublin 2
   Ireland

   Phone: +353-1-896-2354
   Email: stephen.farrell@cs.tcd.ie