Use of TLS for Email Submission and Access

draft-ietf-uta-tls-for-email-03

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 April 24, 2020.

Copyright Notice

Copyright (c) 2019 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
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 Due to the deprecation of TLS 1.1 in [I-D.ietf-tls-oldversions-deprecate], this recommendation is no longer valid.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 1.1 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 and Viktor Dukhovni for their feedback.

7. References

7.1. Informative References

7.2. Normative References

[I-D.ietf-tls-oldversions-deprecate]


Authors’ Addresses

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

Phone: +230 59762817
Email: logan@cyberstorm.mu

Stephen Farrell
Trinity College Dublin
Dublin  2
Ireland

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