Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 25, 2019

L. Velvindron
cyberstorm.mu
S. Farrell
Trinity College Dublin

September 21, 2018

Use of Transport Layer Security (TLS) for Email Submission and Access
draft-lvelvindron-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 March 25, 2019.

Table of Contents

1. Introduction

[RFC8314] defines the minimum recommended for TLS as version 1.1. Due to the deprecation of TLS 1.1 in draft-ietf-tls-oldversions-deprecate, this recommendation is no longer valid.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. Updates to RFC8314

In the Table of contents section, the text should be revised from: "4.1. Deprecation of Services Using Cleartext and TLS Versions Less Than 1.1" to: "4.1. Deprecation of Services Using Cleartext and TLS Versions Less Than 1.2"

In section 4, the text should be revised from: "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." to: "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 1.2 or later and discontinue support for those earlier versions of SSL and TLS."

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." to: "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."

In section 5, the text should be revised from: " MUAs SHOULD provide a prominent indication of the level of confidentiality associated with an account configuration that is appropriate for the user interface (for example, a "lock" icon or changed background color for a visual interface, or some sort of audible indication for an audio

user interface), at appropriate times and/or locations, in order to inform the user of the confidentiality of the communications associated with that account. For example, this might be done whenever (a) the user is prompted for authentication credentials, (b) the user is composing mail that will be sent to a particular submission server, (c) a list of accounts is displayed (particularly if the user can select from that list to read mail), or (d) the user is asking to view or update any configuration data that will be stored on a remote server. 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. " to: " MUAs SHOULD provide a prominent indication of the level of confidentiality associated with an account configuration that is appropriate for the user interface (for example, a "lock" icon or changed background color for a visual interface, or some sort of audible indication for an audio user interface), at appropriate times and/or locations, in order to inform the user of the confidentiality of the communications associated with that account. For example, this might be done whenever (a) the user is prompted for authentication credentials, (b) the user is composing mail that will be sent to a particular submission server, (c) a list of accounts is displayed (particularly if the user can select from that list to read mail), or (d) the user is asking to view or update any configuration data that will be stored on a remote server. 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. "

In Section 5 the text should be revised from: " 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. " to: " 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 1.2 [RFC5246] when accessing accounts that are configured to impose minimum confidentiality requirements. "

In Section 5.2 second paragraph, the text should be revised from: " 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. " to: " 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. "

3. IANA Considerations

None of the proposed measures have an impact on IANA.

4. Security Considerations

The purpose of this document is to document updated recommendations for using TLS with Email services.

5. Normative References

[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>.

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