Internet Engineering Task Force
Internet-Draft
Updates: 5425 6012 (if approved)
Intended status: Standards Track
Expires: 2 August 2022

C. Lonvick
S. Turner
sn3rd
J. Salowey
Salesforce

29 January 2022

Updates to the Cipher Suites in Secure Syslog
draft-ciphersuites-in-sec-syslog-01

Abstract

This document updates the cipher suites in RFC 5425, Transport Layer Security (TLS) Transport Mapping for Syslog, and RFC 6012, Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog. It also updates the transport protocol in RFC 6012.

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 2 August 2022.

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 3
3. Support for Updating 3
4. Updates to RFC 5425 4
5. Updates to RFC 6012 4
6. Authors Notes 5
7. Acknowledgments 5
8. IANA Considerations 6
9. Security Considerations 6
10. References 6
10.1. Normative References 6
10.2. Informative References 7
Authors' Addresses 8

1. Introduction

The Syslog Working Group produced Transport Layer Security (TLS) Transport Mapping for Syslog [RFC5425] and Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog [RFC6012].

Both [RFC5425] and [RFC6012] MUST support certificates as defined in [RFC5280].

[RFC5425] requires that implementations "MUST" support TLS 1.2 [RFC5246] and are "REQUIRED" to support the mandatory to implement cipher suite TLS_RSA_WITH_AES_128_CBC_SHA (Section 4.2).

[RFC6012] requires that implementations "MUST" support DTLS 1.0 [RFC4347] and are also "REQUIRED" to support the mandatory to implement cipher suite TLS_RSA_WITH_AES_128_CBC_SHA (Section 5.2).

The TLS_RSA_WITH_AES_128_CBC_SHA cipher suite has been found to be

weak and the community is moving away from it and towards more robust suites.

The DTLS 1.0 transport [RFC4347] has been deprecated by [BCP195] and the community is moving to DTLS 1.2 [RFC6347] and DTLS 1.3 [I-D.ietf-tls-dtls13].

This document updates [RFC5425] and [RFC6012] to deprecate the use of TLS_RSA_WITH_AES_128_CBC_SHA and to make new recommendations to a mandatory to implement cipher suite to be used for implementations. This document also updates [RFC6012] to make a recommendation of a mandatory to implement secure datagram transport.

2. Terminology

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. Support for Updating

[I-D.salowey-tls-rfc8447bis] generally reminds us that cryptographic algorithms and parameters will be broken or weakened over time. Blindly implementing the cryptographic algorithms listed in any specification is not advised. Implementers and users need to check that the cryptographic algorithms specified continue to provide the expected level of security.

As the Syslog Working Group determined, Syslog clients and servers MUST use certificates as defined in [RFC5280]. Since both [RFC5425] and [RFC6012] REQUIRE the use of TLS_RSA_WITH_AES_128_CBC_SHA, it is very likely that RSA certificates have been implemented in devices adhering to those specifications. [BCP195] notes that ECDHE cipher suites exist for both RSA and ECDSA certificates, so moving to an ECDHE cipher suite will not require replacing or moving away from any currently installed RSA-based certificates.

[I-D.saviram-tls-deprecate-obsolete-kex] documents that the cipher suite TLS_RSA_WITH_AES_128_CBC_SHA has been found to be weak. As such, the community is moving away from that and other weak suites and towards more robust suites such as TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, which is also listed as a currently Recommended algorithm in [I-D.salowey-tls-rfc8447bis].

Along those lines, [I-D.ietf-uta-rfc7525bis] notes that TLS_RSA_WITH_AES_128_CBC_SHA does not provide forward secrecy, a feature that is highly desirable in securing event messages. That document also goes on to recommend TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as a cipher suite that does provide forward secrecy.

Therefore, the mandatory to implement cipher suites listed in [RFC5425] and [RFC6012] must be updated so that implementations of secure syslog are still considered to provide an acceptable and expected level of security.

Additionally, [BCP195] [RFC8996] deprecates the use of DTLS 1.0 [RFC4347], which is the mandatory to implement transport protocol for [RFC6012]. Therefore, the transport protocol for [RFC6012] must be updated.

4. Updates to RFC 5425

Implementations of [RFC5425] MUST NOT offer TLS_RSA_WITH_AES_128_CBC_SHA. The mandatory to implement cipher suite is REQUIRED to be TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

Implementations of [RFC5425] MUST continue to use TLS 1.2 [RFC5246] as the mandatory to implement transport protocol.

Implementations of [RFC5425] MAY use TLS 1.3 [RFC8446] as a transport as long as they support the currently recommended cipher suites.

EDITOR's NOTE: Need to address 0-RTT considerations.

5. Updates to RFC 6012

Implementations of [RFC6012] MUST NOT offer TLS_RSA_WITH_AES_128_CBC_SHA. The mandatory to implement cipher suite is REQUIRED to be TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

As specified in [BCP195], implementations of [RFC6012] must not use DTLS 1.0 [RFC4347]. Implementations MUST use DTLS 1.2 [RFC6347].

DTLS 1.2 [RFC6347] implementations are REQUIRED to support the mandatory to implement cipher suite, which is TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

Implementations of [RFC6012] MAY use DTLS 1.3 [I-D.ietf-tls-dtls13] as a transport as long as they support the currently recommended cipher suites.

EDITOR's NOTE: Need to address 0-RTT considerations.

6. Authors Notes

This section will be removed prior to publication.

This is version -01. Comments were received regarding the -00 version that this document should not imply that the use of DTLS1.0 is being deprecated by this I-D since that was done by RFC 8996. Edits have been made to clarify that. Also, the authors want this document to update RFC 6012 because it says more about cipher suites than RFC 8996 and, since there will be 1.3, we're saying ya' gotta use 1.2 (for now).

Members of IEC 62351 TC 57 WG15, who prompted this work, have proposed the following text to be inserted into their documents.

> The selection of TLS connection parameters such as cipher suites, session resumption and renegotiation shall be reused from IEC 62351-3 specification. Note that port TCP/6514 is assigned by IANA to RFC 5425 (syslog-tls). The RFC requires the support of TLS1.2 and a SHA-1 based cipher suite, but does not mandate its

| use. The cipher does not align with IEC 62351-3 Ed.2 for profiling TLS. Nevertheless, RFC 5425 does not rule out to use stronger cipher suites. With this, clients and server supporting the selection of cipher suites stated in IEC 62351-3 Ed2 will not experience interoperability problems. Caution has to be taken in environments in which interworking with existing services utilizing syslog over TLS is intended. For these, the syslog server needs to be enabled to support the required cipher suites. This ensures connectivity with clients complying to this document and others complying to RFC 5425. Note that meanwhile the work on an update of RFC 5425 and RFC 6012 has started. It targets the adoption of stronger cipher suites for TLS and DTLS to protect syslog communication.

Comments on this text are welcome.

7. Acknowledgments

The authors would like to thank Arijit Kumar Bose, Steffen Fries and the members of IEC TC57 WG15 for their review, comments, and suggestions. The authors would also like to thank Tom Petch and Juergen Schoenwaelder for their comments and constructive feedback.

8. IANA Considerations

This document makes no requests to IANA.

9. Security Considerations

[BCP195] deprecates an insecure DTLS transport protocol from [RFC6012] and deprecates insecure cipher suits from [RFC5425] and [RFC6012]. This document specifies mandatory to implement cipher suites to those RFCs and the latest version of the DTLS protocol to [RFC6012].

10. References

10.1. Normative References

[BCP14] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017.

<https://www.rfc-editor.org/info/bcp14>

[BCP195] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, May 2015.

Moriarty, K. and S. Farrell, "Deprecating TLS 1.0 and TLS 1.1", BCP 195, RFC 8996, March 2021.

<https://www.rfc-editor.org/info/bcp195>

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, DOI 10.17487/RFC4347, April 2006, <https://www.rfc-editor.org/info/rfc4347>.

[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>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC5425] Miao, F., Ed., Ma, Y., Ed., and J. Salowey, Ed., "Transport Layer Security (TLS) Transport Mapping for Syslog", RFC 5425, DOI 10.17487/RFC5425, March 2009, <https://www.rfc-editor.org/info/rfc5425>.

[RFC6012] Salowey, J., Petch, T., Gerhards, R., and H. Feng, "Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog", RFC 6012, DOI 10.17487/RFC6012,

October 2010, <https://www.rfc-editor.org/info/rfc6012>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[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>.

10.2. Informative References

[I-D.ietf-tls-dtls13]
Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-dtls13, 30 April 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-dtls13>.

[I-D.ietf-uta-rfc7525bis]
Sheffer, Y., Holz, R., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", Work in Progress, Internet-Draft, draft-ietf-uta-rfc7525bis-04, 2 December 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-uta-rfc7525bis-04>.

[I-D.salowey-tls-rfc8447bis]
Salowey, J. and S. Turner, "IANA Registry Updates for TLS and DTLS", Work in Progress, Internet-Draft, draft-salowey-tls-rfc8447bis-01, 2 December 2021, <https://datatracker.ietf.org/doc/html/draft-salowey-tls-rfc8447bis-01>.

[I-D.saviram-tls-deprecate-obsolete-kex]

Aviram, N., "Deprecating Obsolete Key Exchange Methods in TLS", Work in Progress, Internet-Draft, draft-aviram-tls-deprecate-obsolete-kex-00, 9 July 2021, <https://datatracker.ietf.org/doc/html/draft-aviram-tls-deprecate-obsolete-kex-00>.

Authors' Addresses

Chris Lonvick

Email: lonvick.ietf@gmail.com

Sean Turner
sn3rd

Email: sean@sn3rd.com

Joe Salowey
Salesforce

Email: joe@salowey.net