

Internet Engineering Task Force
Internet-Draft
Updates: [5425](#) [6012](#) (if approved)
Intended status: Standards Track
Expires: 24 March 2024

C. Lonvick

S. Turner
sn3rd
J. Salowey
Venafi
21 September 2023

**Updates to the Cipher Suites in Secure Syslog
draft-ietf-uta-ciphersuites-in-sec-syslog-05**

Abstract

The Syslog Working Group published two specifications, namely [RFC 5425](#) and [RFC 6012](#), for securing the Syslog protocol using TLS and DTLS, respectively.

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 24 March 2024.

Copyright Notice

Copyright (c) 2023 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.	Terminology	3
3.	Support for Updating	3
4.	Updates to RFC 5425	4
5.	Updates to RFC 6012	4
6.	Early Data	5
7.	Authors Notes	5
8.	Acknowledgments	5
9.	IANA Considerations	5
10.	Security Considerations	6
11.	References	6
11.1.	Normative References	6
11.2.	Informative References	7
	Authors' Addresses	8

[1.](#) Introduction

The Syslog Working Group published [RFC 5425](#), Transport Layer Security (TLS) Transport Mapping for Syslog, and [RFC 6012](#), Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog.

Both specifications, [[RFC5425](#)] and [[RFC6012](#)], require the use of RSA-based certificates and the use of out-of-date TLS/DTLS versions.

[[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 [[RFC9147](#)].

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

[[draft-ietf-tls-rfc8447bis-04](#)] 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](#)] REQUIRED 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.

[[draft-ietf-tls-deprecate-obsolete-kex-02](#)] 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 [[draft-ietf-tls-rfc8447bis-04](#)].

Along those lines, [[BCP195](#)] [[RFC9325](#)] 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.

Finally, [BCP195] [RFC9325] provides guidance on the support of [[RFC8446] and [RFC9147].

4. Updates to [RFC 5425](#)

Implementations of [RFC5425] SHOULD 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.

As per [BCP195], implementations of [RFC5425] SHOULD support TLS 1.3 [RFC8446] and, if implemented, MUST prefer to negotiate TLS 1.3 over earlier versions of TLS.

5. Updates to [RFC 6012](#)

Implementations of [RFC6012] SHOULD 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.

As per [BCP195], implementations of [RFC6012] SHOULD support DTLS 1.3 [RFC9147] and, if implemented, MUST prefer to negotiate DTLS version 1.3 over earlier versions of DTLS.

6. Early Data

Early data (aka 0-RTT data) is a mechanism defined in TLS 1.3 [RFC8446] that allows a client to send data ("early data") as part of the first flight of messages to a server. Early data is permitted by TLS 1.3 when the client and server share a PSK, either obtained externally or via a previous handshake. The client uses the PSK to authenticate the server and to encrypt the early data.

As noted in Section 2.3 of [draft-ietf-tls-rfc8446bis-09], 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 are no protections against the replay of early data between connections. Appendix E.5 of [draft-ietf-tls-rfc8446bis-09] requires applications not use early data without a profile that defines its use. Because syslog does not support replay protection, see Section 8.4 of [RFC5424]", and most implementations establish a long-lived connection, this document specifies that implementations MUST NOT use early data.

7. Authors Notes

This section will be removed prior to publication.

This is version -05 for the UTA Working Group. These edits reflect comments from the WGLC discussions.

This version changed the MUST NOTs to SHOULD NOTs in Sections 4 and 5. This better conforms with BCP 195 and does not break interoperability from clients that may not yet have been upgraded to current MTI cipher suites.

The Security Considerations section has been updated to reflect this.

8. 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, Juergen Schoenwaelder, Hannes Tschofenig, and Viktor Dukhovni for their comments and constructive feedback.

9. IANA Considerations

This document makes no requests to IANA.

10. Security Considerations

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

The insecure cipher suites SHOULD NOT be offered. If a device currently only has an insecure cipher suite, an administrator of the network should evaluate the conditions and determine if the insecure cipher suite should be allowed so that syslog messages may continue to be delivered until the device is updated to have a secure cipher suite.

11. References

11.1. 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.
- 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](#), November 2022.
- <<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>>.
- [RFC5424] Gerhards, R., "The Syslog Protocol", [RFC 5424](#), March 2009, <<http://www.rfc-editor.org/rfc/rfc5424.txt>>.
- [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>>.
- [RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", [RFC 9147](#), DOI 10.17487/RFC9147, April 2022, <<https://www.rfc-editor.org/info/rfc9147>>.

11.2. Informative References

- [[draft-ietf-tls-deprecate-obsolete-kex-02](#)]
Bartle, C. and N. Aviram, "Deprecating Obsolete Key Exchange Methods in TLS", Work in Progress, Internet-Draft, [draft-ietf-tls-deprecate-obsolete-kex-02](#), 11 July 2023, <<https://www.ietf.org/archive/id/draft-ietf-tls-deprecate-obsolete-kex-02.txt>>.

[[draft-ietf-tls-rfc8446bis-09](#)]

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://www.ietf.org/archive/id/draft-ietf-tls-rfc8446bis-09.txt>>.

[[draft-ietf-tls-rfc8447bis-04](#)]

Salowey, J. A. and S. Turner, "IANA Registry Updates for TLS and DTLS", Work in Progress, Internet-Draft, [draft-ietf-tls-rfc8447bis-04](#), 28 March 2023, <<https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8447bis-04>>.

Authors' Addresses

Chris Lonvick
Email: lonvick.ietf@gmail.com

Sean Turner
sn3rd
Email: sean@sn3rd.com

Joe Salowey
Venafi
Email: joe@salowey.net

