Internet Engineering Task Force (IETF)
Request for Comments: 9662
Updates: 5425, 6012
Category: Standards Track
ISSN: 2070-1721

C. Lonvick

S. Turner
sn3rd

J. Salowey
Venafi

October 2024

Updates to the Cipher Suites in Secure Syslog

Abstract

RFCs 5425 and 6012 describe using TLS and DTLS to securely transport syslog messages. This document updates the cipher suites required by RFC 5245 (TLS Transport Mapping for Syslog) and RFC 6012 (DTLS Transport Mapping for Syslog). It also updates the protocol recommended by RFC 6012 for secure datagram transport.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9662.

Table of Contents

Authors' Addresses

1. Introduction

"Transport Layer Security (TLS) Transport Mapping for Syslog" [RFC5425] and "Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog" [RFC6012] describe using TLS and DTLS to securely transport syslog messages. Both of these specifications require the use of RSA-based certificates and the use of TLS and DTLS versions that are not the most recent.

Section 4.2 of [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 5.2 of [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.

The community is moving away from cipher suites that do not offer forward secrecy and towards more robust suites.

The DTLS 1.0 transport [RFC4347] has been deprecated by RFC 8996 [BCP195], and the community is moving to DTLS 1.2 [RFC6347] and DTLS 1.3 [RFC9147].

This document updates [RFC5425] and [RFC6012] to prefer the use of TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 over the use of TLS_RSA_WITH_AES_128_CBC_SHA.

This document also updates [RFC6012] by recommending 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

[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] 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. RFC 9325 [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.

[DEPRECATE-KEX] documents that the cipher suite TLS_RSA_WITH_AES_128_CBC_SHA, along with some other cipher suites, may require mitigation techniques to achieve expected security, which may be difficult to effectively implement. Along those lines, RFC 9325 [BCP195] 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.

As such, the community is moving away from algorithms that do not provide forward secrecy. For example, the International Electrotechnical Commission (IEC) has selected more robust suites such as TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, which is also listed as a currently RECOMMENDED algorithm in [RFC8447bis] for their deployments of secure syslog.

Additionally, RFC 8996 [BCP195] deprecates the use of DTLS 1.0 [RFC4347], which is the mandatory-to-implement transport protocol per [RFC6012]. Therefore, that transport protocol must be updated.

Finally, RFC 9325 [BCP195] provides guidance on the support of TLS 1.3 [RFC8446] and DTLS 1.3 [RFC9147].

Therefore, to maintain interoperability across implementations, the mandatory-to-implement cipher suites listed in [RFC5425] and [RFC6012] should be updated so that implementations of secure syslog will still interoperate and provide an acceptable and expected level of security.

However, since there are many implementations of syslog using the cipher suites mandated by [RFC6012], a sudden change is not desirable. To accommodate a migration path, TLS_RSA_WITH_AES_128_CBC_SHA or TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 may be used, but it is REQUIRED that TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 be preferred.

4. Updates to RFC 5425

The mandatory-to-implement cipher suites are REQUIRED to be TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_RSA_WITH_AES_128_CBC_SHA.

Implementations of [RFC5425] SHOULD offer TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 but MAY offer TLS_RSA_WITH_AES_128_CBC_SHA.

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

As per RFC 9325 [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

The mandatory-to-implement cipher suites are REQUIRED to be TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_RSA_WITH_AES_128_CBC_SHA.

Implementations of [RFC6012] SHOULD offer TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 but MAY offer TLS_RSA_WITH_AES_128_CBC_SHA.

As specified in RFCs 8996 and 9325 [BCP195], implementations of [RFC6012] MUST NOT use DTLS 1.0 [RFC4347]. Implementations MUST use DTLS 1.2 [RFC6347].

DTLS 1.2 [RFC6347] implementations SHOULD support and prefer the mandatory-to-implement cipher suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

As per RFC 9325 [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 [RFC8446bis], 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 [RFC8446bis] requires that 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. IANA Considerations

This document has no IANA actions.

8. Security Considerations

RFCs 8996 and 9325 [BCP195] deprecate an insecure DTLS transport protocol from [RFC6012] and deprecate insecure cipher suites from [RFC5425] and [RFC6012]. However, the installed base of syslog implementations is not easily updated to immediately adhere to those changes.

This document updates the mandatory-to-implement cipher suites to allow for a migration from TLS_RSA_WITH_AES_128_CBC_SHA to TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 without deprecating the former. Implementations should prefer to use TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

If a device currently only has TLS_RSA_WITH_AES_128_CBC_SHA, an administrator of the network should evaluate the conditions and determine if TLS_RSA_WITH_AES_128_CBC_SHA should be allowed so that syslog messages may continue to be delivered until the device is updated to have TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

9. References

9.1. Normative References

[BCP195] Best Current Practice 195, <https://www.rfc-editor.org/info/bcp195>. At the time of writing, this BCP comprises the following:

Moriarty, K. and S. Farrell, "Deprecating TLS 1.0 and TLS 1.1", BCP 195, RFC 8996, DOI 10.17487/RFC8996, March 2021, <https://www.rfc-editor.org/info/rfc8996>.

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, DOI 10.17487/RFC9325, November 2022, <https://www.rfc-editor.org/info/rfc9325>.

[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>.

[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, DOI 10.17487/RFC5424, March 2009, <https://www.rfc-editor.org/info/rfc5424>.

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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>.

9.2. Informative References

[DEPRECATE-KEX]
Bartle, C. and N. Aviram, "Deprecating Obsolete Key Exchange Methods in TLS 1.2", Work in Progress, Internet-Draft, draft-ietf-tls-deprecate-obsolete-kex-05, 3 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-deprecate-obsolete-kex-05>.

[RFC8446bis]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8446bis-11, 14 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8446bis-11>.

[RFC8447bis]

Salowey, J. A. and S. Turner, "IANA Registry Updates for TLS and DTLS", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8447bis-09, 30 April 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8447bis-09>.

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, Viktor Dukhovni, and the IESG members for their comments and constructive feedback.

Authors' Addresses

Chris Lonvick
Email: lonvick.ietf@gmail.com

Sean Turner
sn3rd
Email: sean@sn3rd.com

Joe Salowey
Venafi
Email: joe@salowey.net