Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 1, 2018

R. Housley
Vigil Security
L. Zieglar
National Security Agency

April 30, 2018

Reclassification of Suite B Documents to Historic Status
draft-housley-suite-b-to-historic-05

Abstract

This document reclassifies the RFCs related to the U.S. National Security Agency (NSA) Suite B cryptographic algorithms as Historic, and it discusses the reasons for doing so. This document moves seven informational RFCs to Historic Status: RFC 5759, RFC 6239, RFC 6318, RFC 6379, RFC 6380, RFC 6403, and RFC 6460. In addition, this document moves three obsolete informational RFCs to Historic Status: RFC 4869, RFC 5008, and RFC 5430.

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 November 1, 2018.

Copyright Notice

Table of Contents

1. Introduction

Several RFCs profile security protocols for use with the National Security Agency (NSA) Suite B Cryptography. Suite B is no longer supported by NSA, and the web pages that specify the cryptographic algorithms are no longer available.

In July 2015, NSA published the Committee for National Security Systems Advisory Memorandum 02-15 as the first step in replacing Suite B with NSA's Commercial National Security Algorithm (CNSA) Suite. Information about the CNSA Suite can be found in [CNSA].

2. Rationale

As indicated in [CNSA], NSA is transitioning from Suite B to the CNSA Suite. As a result, the profiles of the security protocols for the Suite B algorithms are now only of historic interest.

3. The RFCs Related to Suite B

Between 2007 and 2012, several Suite-B-related RFCs were published to profile security protocols for use with the Suite B algorithms. They are:

- [RFC4869], "Suite B Cryptographic Suites for IPsec" (Obsoleted by RFC 6379)
- [RFC5008], "Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)" (Obsoleted by RFC 6318)
- [RFC5430], "Suite B Profile for Transport Layer Security (TLS)" (Obsoleted by RFC 6460)
- [RFC5759], "Suite B Certificate and Certificate Revocation List (CRL) Profile"
- [RFC6239], "Suite B Cryptographic Suites for Secure Shell (SSH)"
- [RFC6318], "Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)"
- [RFC6379], "Suite B Cryptographic Suites for IPsec"
- [RFC6380], "Suite B Profile for Internet Protocol Security (IPsec)"
- [RFC6403], "Suite B Profile of Certificate Management over CMS"
- [RFC6460], "Suite B Profile for Transport Layer Security (TLS)"

4. Documents that Reference the Suite-B-related RFCs

There are several references among these RFCs. These cross-references are not examined further.

Other RFC make reference to these Suite-B-related RFCs; these references are discussed in the following subsections.

4.1. Documents that Reference RFC 4869

One other RFC makes reference to RFC 4869 [RFC4869].

RFC 6071, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap" [RFC6071], points out that RFC 4869 adds four pre-defined suites based upon Suite B specifications. They are:

- IKE/ESP suite "Suite-B-GCM-128"
- IKE/ESP suite "Suite-B-GCM-256"
- IKE/AH suite "Suite-B-GMAC-128"

o IKE/AH suite "Suite-B-GMAC-256"

In each case, these suite definitions make use of algorithms that are defined in other RFCs. No interoperability or security concerns are raised if implementations continue to make use of these suite names.

4.2. Documents that Reference RFC 5759

One other RFC makes reference to RFC 5759 [RFC5759].

RFC 6187, "X.509v3 Certificates for Secure Shell Authentication" [RFC6187], points out that RFC 5759 provides additional guidance for Elliptic Curve Digital Signature Algorithm (ECDSA) keys when used with Suite B.

4.3. Documents that Reference RFC 6379

One other RFC makes reference to RFC 6379 [RFC6379].

RFC 7321, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH) [RFC7321], points out that the AES-GCM algorithm is used by Suite B, and it has emerged as the preferred authenticated encryption method in IPsec.

4.4. Documents that Reference RFC 6403

Two other RFCs make reference to RFC 6403 [RFC6403].

RFC 6402, "Certificate Management over CMS (CMC) Updates" [RFC6402], says that development of the profile for Suite B was the activity that demonstrated the need for these updates.

RFC 7030, "Enrollment over Secure Transport" [RFC7030], points out that the scenarios in the two documents are very similar.

4.5. Documents that Reference RFC 6460

Three other RFCs make reference to RFC 6460 [RFC6460].

RFC 6605, "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC" [RFC6605], states that material was copied liberally from RFC 6460. The standards-track status of RFC 6605 is not affected by RFC 6460 moving to Historic status.

RFC 7525, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)" [RFC7525],

observes that the Suite B profile of TLS 1.2 uses different cipher suites.

RFC 8253, "PCEPS: Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)" [RFC8253], points RFC 6460 for the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suites. Both of these ciphersuites are defined in [RFC5289], which would have been a better reference. The standards-track status of RFC 8253 is not affected by RFC 6460 moving to Historic status.

5. Impact of Reclassifying the Suite-B-related RFCs to Historic

No interoperability or security concerns are raised by reclassifying the Suite-B-related RFCs to Historic Status. As described in Section 4, none of the RFCs being moved to Historic Status is the sole specification of a cryptographic algorithm or an identifier for a cryptographic algorithm.

6. IANA Considerations

No changes are requested to any IANA registries.

7. Security Considerations

No interoperability or security concerns raised by reclassifying the Suite-B-related RFCs to Historic Status.

NSA is transitioning away from some of the cryptographic algorithms and key sizes that were employed in the Suite B profiles.

8. References

8.1. Normative References

[RFC4869] Law, L. and J. Solinas, "Suite B Cryptographic Suites for IPsec", RFC 4869, DOI 10.17487/RFC4869, May 2007, <https://www.rfc-editor.org/info/rfc4869>.

[RFC5008] Housley, R. and J. Solinas, "Suite B in Secure/ Multipurpose Internet Mail Extensions (S/MIME)", RFC 5008, DOI 10.17487/RFC5008, September 2007, <https://www.rfc-editor.org/info/rfc5008>.

[RFC5430] Salter, M., Rescorla, E., and R. Housley, "Suite B Profile for Transport Layer Security (TLS)", RFC 5430, DOI 10.17487/RFC5430, March 2009, <https://www.rfc-editor.org/info/rfc5430>.

[RFC5759] Solinas, J. and L. Zieglar, "Suite B Certificate and Certificate Revocation List (CRL) Profile", RFC 5759, DOI 10.17487/RFC5759, January 2010, <https://www.rfc-editor.org/info/rfc5759>.

[RFC6239] Igoe, K., "Suite B Cryptographic Suites for Secure Shell (SSH)", RFC 6239, DOI 10.17487/RFC6239, May 2011, <https://www.rfc-editor.org/info/rfc6239>.

[RFC6318] Housley, R. and J. Solinas, "Suite B in Secure/ Multipurpose Internet Mail Extensions (S/MIME)", RFC 6318, DOI 10.17487/RFC6318, June 2011, <https://www.rfc-editor.org/info/rfc6318>.

[RFC6379] Law, L. and J. Solinas, "Suite B Cryptographic Suites for IPsec", RFC 6379, DOI 10.17487/RFC6379, October 2011, <https://www.rfc-editor.org/info/rfc6379>.

[RFC6380] Burgin, K. and M. Peck, "Suite B Profile for Internet Protocol Security (IPsec)", RFC 6380, DOI 10.17487/RFC6380, October 2011, <https://www.rfc-editor.org/info/rfc6380>.

[RFC6403] Zieglar, L., Turner, S., and M. Peck, "Suite B Profile of Certificate Management over CMS", RFC 6403, DOI 10.17487/RFC6403, November 2011, <https://www.rfc-editor.org/info/rfc6403>.

[RFC6460] Salter, M. and R. Housley, "Suite B Profile for Transport Layer Security (TLS)", RFC 6460, DOI 10.17487/RFC6460, January 2012, <https://www.rfc-editor.org/info/rfc6460>.

8.2. Informative References

[CNSA] National Security Agency, "Commercial National Security Algorithm (CNSA) Suite", 2015, <https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm>.

[RFC5289] Rescorla, E., "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)", RFC 5289, DOI 10.17487/RFC5289, August 2008, <https://www.rfc-editor.org/info/rfc5289>.

[RFC6071] Frankel, S. and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", RFC 6071, DOI 10.17487/RFC6071, February 2011, <https://www.rfc-editor.org/info/rfc6071>.

[RFC6187] Igoe, K. and D. Stebila, "X.509v3 Certificates for Secure Shell Authentication", RFC 6187, DOI 10.17487/RFC6187, March 2011, <https://www.rfc-editor.org/info/rfc6187>.

[RFC6402] Schaad, J., "Certificate Management over CMS (CMC) Updates", RFC 6402, DOI 10.17487/RFC6402, November 2011, <https://www.rfc-editor.org/info/rfc6402>.

[RFC6605] Hoffman, P. and W. Wijngaards, "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC", RFC 6605, DOI 10.17487/RFC6605, April 2012, <https://www.rfc-editor.org/info/rfc6605>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/info/rfc7030>.

[RFC7321] McGrew, D. and P. Hoffman, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 7321, DOI 10.17487/RFC7321, August 2014, <https://www.rfc-editor.org/info/rfc7321>.

[RFC7525] 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, DOI 10.17487/RFC7525, May 2015, <https://www.rfc-editor.org/info/rfc7525>.

[RFC8253] Lopez, D., Gonzalez de Dios, O., Wu, Q., and D. Dhody, "PCEPS: Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)", RFC 8253, DOI 10.17487/RFC8253, October 2017, <https://www.rfc-editor.org/info/rfc8253>.

Authors' Addresses

Russ Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
US

Email: housley@vigilsec.com

Lydia Zieglar
National Security Agency
9800 Savage Road
Ft. George G. Meade, MD 20755-6940
US

Email: llziegl@nsa.gov