Internet Engineering Task Force (IETF)
Request for Comments: 8423
Category: Informational
ISSN: 2070-1721

R. Housley
Vigil Security
L. Zieglar
National Security Agency

July 2018

Перевод документов Suite B в статус Historic

Reclassification of Suite B Documents to Historic Status

Тезисы

Этот документ переводит RFC, относящиеся к набору криптографических алгоритмов Suite B Агентства национальной безопасности США (NSA[1]), в статус устаревших (Historic) и рассматривает причины этого. Документ переводит в число устаревших информационные RFC 5759, 6239, 6318, 6379, 6380, 6403 и 6460. Кроме того, в статус Historic переводятся три отмененных (obsoleted) информационных RFC 4869, 5008 и 5430.

Статус документа

Документ не содержит спецификации Internet Standards Track и публикуется с информационными целями.

Документ является результатом работы IETF[2] и представляет согласованный взгляд сообщества IETF. Документ прошел открытое обсуждение и был одобрен для публикации IESG[3]. Не все документы, одобренные IESG, претендуют на статус стандартов Internet, как указано в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc8423.

Оглавление

1. Введение

Несколько RFC задавали профили протоколов защиты для использования с криптографией АНБ Suite B. Алгоритмы Suite B больше не поддерживаются АНБ и web-страницы со спецификациями этих криптографических алгоритмов больше не доступны.

А июле 2015 года АНБ опубликовало Committee for National Security Systems Advisory Memorandum 02-15 в качестве первого шага по замене алгоритмов Suite B алгоритмами набора CNSA[4]. Информацию об этих алгоритмах можно найти в [CNSA].

[1]United States National Security Agency.
[2]Internet Engineering Task Force.
[3]Internet Engineering Steering Group.
[4]Commercial National Security Algorithm — коммерческий алгоритм национальной безопасности.

2. Обоснование

Как указано в [CNSA], АНБ переходит с алгоритмов Suite B к алгоритмам CNSA. В результате профили протоколов защиты для алгоритмов Suite B в дальнейшем представляют лишь исторический интерес.

3. RFC, относящиеся к Suite B

В интервале с 2007 г. по 2012 г. было опубликовано несколько относящихся к Suite B документов RFCs с профилями протоколов защиты, использующих алгоритмы Suite B. Эти документы перечислены ниже.

- [RFC4869], "Suite B Cryptographic Suites for IPsec" (отменен RFC 6379).
- [RFC5008], "Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)" (отменен RFC 6318).
- [RFC5430], "Suite B Profile for Transport Layer Security (TLS)" (отменен 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. Документы, ссылающиеся на связанные с Suite B RFC

Эти RFC неоднократно ссылаются один на другой. Такие перекрестные ссылки далее в этом документе не рассматриваются.

В других RFC также имеются ссылки на связанные с Suite B RFC, эти ссылки рассматриваются в следующих параграфах.

4.1. Документы со ссылками на RFC 4869

В одном RFC имеется ссылка на RFC 4869 [RFC4869].

RFC 6071, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap" [RFC6071] указывает, что RFC 4869 добавляет 4 предопределенных шифра на основе спецификаций Suite B:

- шифр IKE/ESP "Suite-B-GCM-128";
- шифр IKE/ESP "Suite-B-GCM-256";
- шифр IKE/ESP "Suite-B-GMAC-128";
- шифр IKE/ESP "Suite-B-GMAC-256".

В каждом случае эти шифры используют алгоритмы, определенные в других RFC. Если реализация продолжает использовать имена этих шифров, каких-либо проблем взаимодействия или безопасности не возникает.

4.2. Документы со ссылками на RFC 5759

В одном RFC имеется ссылка на RFC 5759 [RFC5759].

RFC 6187, "X.509v3 Certificates for Secure Shell Authentication" [RFC6187] указывает, что RFC 5759 содержит дополнительные рекомендации для использования ключей ECDSA[1] с Suite B.

4.3. Документы со ссылками на RFC 6379

В одном RFC имеется ссылка на RFC 6379 [RFC6379].

RFC 7321, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)" [RFC7321] указывает, что алгоритм AES-GCM используется в Suite B и этот алгоритм стал предпочтительным методом аутентифицированного шифрования в IPsec. RFC 7321 был отменен RFC 8221.

4.4. Документы со ссылками на RFC 6403

В двух RFC имеются ссылки на RFC 6403 [RFC6403].

RFC 6402, "Certificate Management over CMS (CMC) Updates" [RFC6402] указывает, что разработка профиля для Suite B показала необходимость внесенных этим документом обновлений.

RFC 7030, "Enrollment over Secure Transport" [RFC7030] указывает, что сценарии из Приложения к RFC 6403 очень похожи на три описанных сценария.

4.5. Документы со ссылками на RFC 6460

В двух RFC имеются ссылки на RFC 6460 [RFC6460].

[1]Elliptic Curve Digital Signature Algorithm — алгоритм цифровой подписи на основе эллиптической кривой.

RFC 6605, "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC" [RFC6605] заявляет о копировании части материала из RFC 6460. Статус Standards Track для RFC 6605 не меняется в результате перевода RFC 6460 в состояние Historic.

RFC 7525, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)" [RFC7525] отмечает, что профиль Suite B для TLS 1.2 использует разные шифронаборы.

RFC 8253, "PCEPS: Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)" [RFC8253] указывает на RFC 6460 для шифронаборов TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 и TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384. Оба эти шифронабора определены в [RFC5289], на который было бы лучше сослаться. Статус Standards Track для RFC 8253 не меняется в результате перевода RFC 6460 в состояние Historic.

5. Влияние перевода связанных с Suite B RFC в статус Historic

Не возникает каких-либо проблем взаимодействия или безопасности в результате перевода связанных с Suite B RFC в статус Historic. Как указано в разделе 4, ни один из переведенных в число устаревших RFC не содержит явной спецификации криптографического алгоритма или идентификатора криптоалгоритма.

6. Взаимодействие с IANA

Документ не требует действий со стороны IANA.

7. Вопросы безопасности

Не возникает каких-либо проблем взаимодействия или безопасности в результате перевода связанных с Suite B RFC в статус Historic.

АНБ отказывается от некоторых криптографических алгоритмов и размеров ключей, которые были использованы в профилях Suite B.

8. Литература

8.1. Нормативные документы

[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. Дополнительная литература

[CNSA] National Security Agency, "Commercial National Security Algorithm Suite", August 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>.

Адреса авторов

Russ Housley

Vigil Security, LLC

918 Spring Knoll Drive

Herndon, VA 20170

United States of America

Email: housley@vigilsec.com

Lydia Zieglar

National Security Agency

9800 Savage Road

Ft. George G. Meade, MD 20755-6940

United States of America

Email: llziegl@nsa.gov

Перевод на русский язык

Николай Малых

nmalykh@gmail.com