Network
Internet-Draft
Updates: 7296 (if approved)
Intended status: Standards Track
Expires: September 12, 2019

P. Wouters, Ed.
Red Hat

March 11, 2019

Deprecation of IKEv1 and obsoleted algorithms
draft-pwouters-ikev1-ipsec-graveyard-00

Abstract

This document deprecates Internet Key Exchange version 1 (IKEv1) and additionally deprecates a number of algorithms that are obsolete.

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 http://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 September 12, 2019.

Table of Contents

1. Introduction

IKEv1 [RFC2409] and its related documents for ISAKMP [RFC2408] and IPsec DOI [RFC2407] were obsoleted by IKEv2 [RFC4306] in December 2005. The latest version of IKEv2 at the time of writing was published in 2014 in [RFC7296]. The Internet Key Exchange (IKE) version 2 has replaced version 1 over 15 years ago. IKEv2 has now seen wide deployment and provides a full replacement for all IKEv1 functionality. No new modifications or new algorithms have been accepted for IKEv1 for at least a decade. IKEv2 addresses various issues present in IKEv1, such as IKEv1 being vulnerable to amplification attacks. This document specifies the deprecation of IKEv1. IKEv1 MUST NOT be deployed.

Algorithm implementation requirements and usage guidelines for IKEv2 [RFC8247] and ESP/AH [RFC8223] gives guidance to implementors but limits that guidance to avoid broken or weak algorithms. It does not deprecate algorithms that have aged and are no longer in use, but leave these algorithms in a state of "MAY be used". This document deprecates those algorithms that are no longer advised but for which there are no known attacks resulting in their earlier deprecation.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Deprecating IKEv1

IKEv1 is deprecated and MUST NOT be deployed. Systems running IKEv1 should be upgraded and reconfigured to run IKEv2. Systems that support IKEv1 but not IKEv2 are most likely also unsuitable candidates for continued operation. Such unsupported systems have a much higher chance of containing an implementation vulnerability that

will never be patched. IKEv1 systems can be abused for packet amplification attacks. IKEv1 systems most likely do not support modern algorithms such as AES-GCM or CHACHA20_POLY1305 and quite often only support or have been configured to use the very weak DiffieHellman Groups 2 and 5. IKEv1 systems must be upgraded or replaced by IKEv2 systems.

IKEv1 and its way of using Preshared Keys (PSKs) protects against quantum computer based attacks. IKEv2 updated its use of PSK to improve the error reporting, but at the expense of post-quantum security. If post-quantum security is required, these systems should be migrated to use IKEv2 Postquantum Preshared Keys (PPK) [draft-ietf-ipsecme-qr-ikev2].

Some IKEv1 implementations support Labeled IPsec, a method to negotiate an addition Security Context selector to the SPD, but this method was never standarized in IKEv1. Those IKEv1 systems that require Labeled IPsec should migrate to an IKEv2 system supporting Labeled IPsec as specified in [draft-ietf-ipsecme-labeled-ipsec].

EDITOR NOTE: This document is expected to be released only after the PPK draft has become an RFC. While the same could be said for Labeled IPsec, there is no IKEv1 RFC that specifies Labeled IPsec, so pointing to a draft here does not demote a reference from RFC to a draft.

4. Deprecating obsolete algorithms

This document deprecates the following algorithms:

- Encryption Algorithms: 1DES, RC5, IDEA, CAST, Blowfish and 3IDEA
- PRF Algorithms: HMAC-MD5
- Integrity Algorithms: HMAC-MD5-96, HMAC-MD5-128 and HMAC-SHA1-160
- Diffie-Hellman groups: 1, 2, 5, 22, 23 and 24

5. Security Considerations

There are only security benefits by deprecating IKEv1 for IKEv2.

The deprecated algorithms have long been in disuse and are no longer actively deployed or researched. It presents an unknown security risk that is best avoided. Additionally, these algorithms not being supported in implementations simplifies those implementations and reduces the accidental use of these deprecated algorithms through misconfiguration or downgrade attacks.

6. IANA Considerations

This document instructs IANA to mark all IKEv1 registries as DEPRECATED.

Additionally, this document instructs IANA to add an additional Status column to the IKEv2 Transform Type registries and mark the following entries as DEPRECATED:

Transform Type 1 - Encryption Algorithm IDs

Number	Name	Status
1	ENCR_DES_IV64	DEPRECATED
2	ENCR_DES	DEPRECATED
4	ENCR_RC5	DEPRECATED
5	ENCR_IDEA	DEPRECATED
6	ENCR_CAST	DEPRECATED
7	ENCR_BLOWFISH	DEPRECATED
8	ENCR_3IDEA	DEPRECATED
9	ENCR_DES_IV32	DEPRECATED

Figure 1

Transform Type 2 - Pseudorandom Function Transform IDs

Number	Name	Status
1	PRF_HMAC_MD5	DEPRECATED

Figure 2

Transform Type 3 - Integrity Algorithm Transform IDs

Number	Name	Status
1	AUTH_HMAC_MD5_96	DEPRECATED
6	AUTH_HMAC_MD5_128	DEPRECATED
7	AUTH_HMAC_SHA1_160	DEPRECATED

Figure 3

Transform Type 4 - Diffie Hellman Group Transform IDs

Number	Name	Status
1	768-bit MODP Group	DEPRECATED
2	1024-bit MODP Group	DEPRECATED
5	1536-bit MODP Group	DEPRECATED
22	1024-bit MODP Group with 160-bit Prime Order Subgroup	DEPRECATED
23	2048-bit MODP Group with 224-bit Prime Order Subgroup	DEPRECATED
24	2048-bit MODP Group with 256-bit Prime Order Subgroup	DEPRECATED

Figure 4

All entries not mentioned here should receive no value in the new Status field.

7. References

7.1. Normative References

[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>.

[RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, DOI 10.17487/RFC2407, November 1998, <https://www.rfc-editor.org/info/rfc2407>.

[RFC2408] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, DOI 10.17487/RFC2408, November 1998, <https://www.rfc-editor.org/info/rfc2408>.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, DOI 10.17487/RFC2409, November 1998, <https://www.rfc-editor.org/info/rfc2409>.

[RFC4306] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, DOI 10.17487/RFC4306, December 2005, <https://www.rfc-editor.org/info/rfc4306>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC8223] Esale, S., Torvi, R., Jalil, L., Chunduri, U., and K. Raza, "Application-Aware Targeted LDP", RFC 8223, DOI 10.17487/RFC8223, August 2017, <https://www.rfc-editor.org/info/rfc8223>.

[RFC8247] Nir, Y., Kivinen, T., Wouters, P., and D. Migault, "Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 8247, DOI 10.17487/RFC8247, September 2017, <https://www.rfc-editor.org/info/rfc8247>.

7.2. Informative References

[draft-ietf-ipsecme-labeled-ipsec]
Wouters, P. and S. Prasad, "Labeled IPsec Traffic Selector support for IKEv2", draft-ietf-ipsecme-labeled-ipsec (work in progress), March 2019.

[draft-ietf-ipsecme-qr-ikev2]
Fluhrer, S., McGre, D., Kampanakis, P., and V. Smyslov, "Postquantum Preshared Keys for IKEv2", draft-ietf-ipsecme-qr-ikev2 (work in progress), January 2019.

Author's Address

Paul Wouters (editor)
Red Hat

Email: pwouters@redhat.com