Workgroup: Network
Internet-Draft:
draft-ietf-ipsecme-ikev1-algo-to-historic-06
Updates: 8221, 8247 (if approved)
Published: 10 June 2022
Intended Status: Standards Track
Expires: 12 December 2022
Authors: P. Wouters, Ed.
Aiven

Deprecation of IKEv1 and obsoleted algorithms

Abstract

Internet Key Exchange version 1 (IKEv1) is deprecated. Accordingly, IKEv1 has been moved to Historic status. A number of old algorithms that are associated with IKEv1, and not widely implemented for IKEv2 are deprecated as well. This document adds a Status column to the IANA IKEv2 Transform Type registries that shows the deprecation status.

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 12 December 2022.

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. IKEv1 has been moved to Historic status.

Algorithm implementation requirements and usage guidelines for IKEv2 [RFC8247] and ESP/AH [RFC8221] gives guidance to implementors but limits that guidance to avoid broken or weak algorithms. It does not deprecate algorithms that have aged and are not 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", "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. RFC2407, RFC2408 and RFC2409 are Historic

IKEv1 is deprecated. 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:

* IKEv1 development ceased over a decade ago and no new work will happen. This poses the risk of unmaintained code in an otherwise supported product which can result in security vulnerabilities.

* A number of IKEv1 systems have reached their End of Life and therefor will never be patched by the vendor if a vulnerability is found.

* There are vendors that still provide updates for their equipment that supports IKEv1 and IKEv2, but have "frozen" their IKEv1 implementation. Such users might not be aware that they are running unmaintained code with its associated security risks.

* IKEv1 systems can be abused for packet amplification attacks, as documented in the Security Bulletin CVE-2016-5361.

* Great strides have been made in cryptography since IKEv1 development ceased. While some modern cryptographic algorithms were added to IKEv1, interoperability concerns mean that the defacto algorithms negotiated by IKEv1 will consist of dated or deprecated algorithms like AES-CBC, SHA1, and Diffie-Hellman groups 1 or 2. IKEv2 provides state-of-the-art suite of cryptographic algorithms that IKEv1 lacks.

IKEv2 is a more secure protocol than IKEv1. For example, IKEv2 offers more modern cryptographic primitives, proper defense against denial of service attacks, improved authentication via EAP methods, PAKE support and is actively worked on with respect to defending against quantum computer attacks.

IKEv1-only systems should be upgraded or replaced by systems supporting IKEv2. IKEv1 configurations SHOULD NOT be directly translated to IKEv2 configurations without updating the cryptographic algorithms used.

4. IKEv1 feature equivalents for IKEv2

A few notably IKEv1 features are not present in the IKEv2 core specification [RFC7296] but are available for IKEv2 via an additional specification:

4.1. IKEv2 postquantum support

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) [RFC8784]

4.2. IKEv2 Labeled IPsec support

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].

4.3. IKEv2 Group SA / Multicast support

The Group Domain of Interpretation (GDOI, [RFC6407]) protocol, based on IKEv1 defines the support for Multicast Group SAs. For IKEv2, this work is currently in progress via [draft-ietf-ipsecme-g-ikev2]

5. Deprecating obsolete algorithms

This document deprecates the following algorithms:

- *Encryption Algorithms: RC5, IDEA, CAST, Blowfish, and the unspecified 3IDEA, ENCR_DES_IV64 and ENCR_DES_IV32

- *PRF Algorithms: the unspecified PRF_HMAC_TIGER

- *Integrity Algorithms: HMAC-MD5-128

- *Diffie-Hellman groups: none

6. 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.

7. IANA Considerations

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 [this document]
2	ENCR_DES	DEPRECATED [RFC8247]
4	ENCR_RC5	DEPRECATED [this document]
5	ENCR_IDEA	DEPRECATED [this document]
6	ENCR_CAST	DEPRECATED [this document]
7	ENCR_BLOWFISH	DEPRECATED [this document]
8	ENCR_3IDEA	DEPRECATED [this document]
9	ENCR_DES_IV32	DEPRECATED [this document]

Figure 1

Transform Type 2 - Pseudorandom Function Transform IDs

Number	Name	Status
1	PRF_HMAC_MD5	DEPRECATED [RFC8247]
1	PRF_HMAC_TIGER	DEPRECATED [this document]

Figure 2

Transform Type 3 - Integrity Algorithm Transform IDs

Number	Name	Status
1	AUTH_HMAC_MD5_96	DEPRECATED [RFC8247]
3	AUTH_DES_MAC	DEPRECATED [RFC8247]
4	AUTH_KPDK_MD5	DEPRECATED [RFC8247]
6	AUTH_HMAC_MD5_128	DEPRECATED [this document]
7	AUTH_HMAC_SHA1_160	DEPRECATED [this document]

Figure 3

Transform Type 4 - Diffie Hellman Group Transform IDs

Number	Name	Status
1	768-bit MODP Group	DEPRECATED [RFC8247]
22	1024-bit MODP Group with 160-bit Prime Order Subgroup	DEPRECATED [RFC8247]

Figure 4

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

8. References

8.1. 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>.

[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>.

[RFC8221] Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 8221, DOI 10.17487/RFC8221, October 2017, <https://www.rfc-editor.org/info/rfc8221>.

[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>.

8.2. Informative References

[draft-ietf-ipsecme-g-ikev2] Smyslov, V. and B. Weis, "Group Key Management using IKEv2", Work in Progress, Internet-Draft, draft-ietf-ipsecme-g-ikev2, 11 January 2021, <https://www.ietf.org/archive/id/draft-ietf-ipsecme-g-ikev2-03.txt>.

[draft-ietf-ipsecme-labeled-ipsec] Wouters, P. and S. Prasad, "Labeled IPsec Traffic Selector support for IKEv2", Work

in Progress, Internet-Draft, draft-ietf-ipsecme-labeled-ipsec, 25 October 2021, <https://tools.ietf.org/id/draft-ietf-ipsecme-labeled-ipsec-06.txt>.

[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>.

[RFC6407] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, DOI 10.17487/RFC6407, October 2011, <https://www.rfc-editor.org/info/rfc6407>.

[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>.

[RFC8784] Fluhrer, S., Kampanakis, P., McGrew, D., and V. Smyslov, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security", RFC 8784, DOI 10.17487/RFC8784, June 2020, <https://www.rfc-editor.org/info/rfc8784>.

Author's Address

Paul Wouters (editor)
Aiven

Email: paul.wouters@aiven.io