Stream: Internet Engineering Task Force (IETF)
RFC: 9395
Updates: 8221, 8247
Category: Standards Track
Published: April 2023
ISSN: 2070-1721

Author: P. Wouters, Ed.
Aiven

RFC 9395
Deprecation of the Internet Key Exchange Version 1 (IKEv1) Protocol and Obsoleted Algorithms

Abstract

Internet Key Exchange Version 1 (IKEv1) has been deprecated, and RFCs 2407, 2408, and 2409 have been moved to Historic status. This document updates RFCs 8221 and 8247 to reflect the usage guidelines of old algorithms that are associated with IKEv1 and are not specified or commonly implemented for IKEv2. This document further updates the IANA registries for IKEv2 "Transform Type Values" by adding a "Status" column where the deprecation status can be listed.

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/rfc9395.

Copyright Notice

Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

IKEv1 has been moved to Historic status. IKEv1 [RFC2409] and its related documents for the Internet Security Association and Key Management Protocol (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 [RFC7296]. Since IKEv2 replaced IKEv1 over 15 years ago, IKEv2 has now seen wide deployment, and it 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.

Algorithm implementation requirements and usage guidelines for IKEv2 [RFC8247] and Encapsulating Security Payload (ESP) and Authentication Header (AH) [RFC8221] gives guidance to implementors but limits that guidance to avoid broken or weak algorithms. These two RFCs do not deprecate algorithms that have aged and are not in use. Instead, they leave these algorithms in a state of "**MAY** be used" by not mentioning them. This document deprecates those unmentioned 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. RFCs 2407, 2408, and 2409 Are Historic

As 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 for the following reasons:

- 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, therefore, 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 a 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 Extensible Authentication Protocol (EAP) methods, and password-authenticated key exchange (PAKE) support. Also, IKEv2 is actively worked on with respect to defending against quantum-computer attacks.

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

4. IKEv1 Feature Equivalents for IKEv2

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

4.1. IKEv2 Post-Quantum Support

IKEv1 and its way of using Preshared Keys (PSKs) protects against quantum-computer-based attacks. IKEv2 updated its use of PSKs 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 Post-quantum Preshared Keys (PPKs) [RFC8784].

4.2. IKEv2 Labeled IPsec Support

Some IKEv1 implementations support Labeled IPsec, a method to negotiate an additional Security Context selector to the Security Policy Database (SPD), but this method was never standardized in IKEv1. Those IKEv1 systems that require Labeled IPsec should migrate to an IKEv2 system supporting Labeled IPsec as specified in [LABELED-IPSEC].

4.3. IKEv2 Group SA and Multicast Support

The Group Domain of Interpretation (GDOI) protocol [RFC6407], which is based on IKEv1, defines the support for Multicast Group SAs. For IKEv2, this work is currently in progress via [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 if IKEv1 is deprecated and IKEv2 is used.

The deprecated algorithms have long been in disuse and are no longer actively deployed or researched; this 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 deprecated algorithms through misconfiguration or downgrade attacks.

7. IANA Considerations

IANA has added the following line at the top of the Notes section of the "Internet Key Exchange (IKE) Attributes" and '"Magic Numbers" for ISAKMP Protocol' registries: "All registries listed below have been closed. See RFC 9395." In addition, this document has been added to the "Reference" column in these two registries, and their registration procedures have been changed to "Registry closed".

IANA has added a "Status" column to the following IKEv2 "Transform Type Values" registries:

Transform Type 1 - Encryption Algorithm Transform IDs

Transform Type 2 - Pseudorandom Function Transform IDs

Transform Type 3 - Integrity Algorithm Transform IDs

Transform Type 4 - Key Exchange Method Transform IDs

Also, the following entries have been marked as DEPRECATED:

Number	Name	Status
1	ENCR_DES_IV64	DEPRECATED (RFC 9395)
2	ENCR_DES	DEPRECATED [RFC8247]
4	ENCR_RC5	DEPRECATED (RFC 9395)
5	ENCR_IDEA	DEPRECATED (RFC 9395)
6	ENCR_CAST	DEPRECATED (RFC 9395)
7	ENCR_BLOWFISH	DEPRECATED (RFC 9395)
8	ENCR_3IDEA	DEPRECATED (RFC 9395)
9	ENCR_DES_IV32	DEPRECATED (RFC 9395)

Table 1: Transform Type 1 - Encryption Algorithm Transform IDs

Number	Name	Status
1	PRF_HMAC_MD5	DEPRECATED [RFC8247]
3	PRF_HMAC_TIGER	DEPRECATED (RFC 9395)

Table 2: Transform Type 2 - Pseudorandom Function 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 (RFC 9395)
7	AUTH_HMAC_SHA1_160	DEPRECATED (RFC 9395)

Table 3: Transform Type 3 - Integrity Algorithm 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]

Table 4: Transform Type 4 - Key Exchange Method Transform IDs

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>.

[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

[CVE-2016-5361] NIST National Vulnerability Database, "CVE-2016-5361 Detail", 16 June 2016, <https://nvd.nist.gov/vuln/detail/CVE-2016-5361>.

[G-IKEV2] Smyslov, V. and B. Weis, "Group Key Management using IKEv2", Work in Progress, Internet-Draft, draft-ietf-ipsecme-g-ikev2-09, 19 April 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-g-ikev2-09>.

[LABELED-IPSEC] Wouters, P. and S. Prasad, "Labeled IPsec Traffic Selector support for IKEv2", Work in Progress, Internet-Draft, draft-ietf-ipsecme-labeled-ipsec-11, 10 April 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-labeled-ipsec-11>.

[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>.

[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>.

[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