Internet Engineering Task Force (IETF)
Internet-Draft
Obsoletes: 4345
Updates: 3501, 4253, 6649, 6733
Intended Status: Best Current Practice
Expires: June 12, 2018

L. Camara

December 9, 2017

Depreciating RC4 in all IETF Protocols
draft-ietf-curdle-rc4-die-die-die-03

[[RFC-Editor: Please replace all instances of xxxx in this document with the RFC number of draft-ietf-curdle-des-des-des-die-die-die.]]

[[RFC-Editor: please replace the second character of my surname by U+00E2 when publishing as RFC in the header and in all pages. Non-ASCII characters are allowed in RFCs as per RFC 7997.]]

Abstract

RC4 is extremely weak as shown by RFC 6649 and RFC 7457, is prohibited in TLS by RFC 7465, is prohibited in Kerberos by RFC xxxx and it needs to be prohibited in all IETF protocols. This document obsoletes RFC 4345 "Improved Arcfour Modes for the Secure Shell (SSH) Transport Layer Protocol" (note Arcfour and RC4 are synonymous). RFC 3501, RFC 4253, RFC 6649 and RFC 6733 are updated to note the deprecation of RC4 in all IETF protocols.

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 June 12, 2018.

Table of Contents

1. Introduction

RC4 is extremely weak [RFC6649] [RFC7457] [RFCxxxx] and this document depreciates its use in all IETF protocols, including Kerberos and Secure Shell (SSH). The reasons for obsoleting RFC 4345 are discussed in Section 2. The updates to RFC 3501, RFC 4253, RFC 6649 and RFC 6733 and the reasons for doing them are specified in sections 3, 4, 5 and 6, respectively.

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 BCP 14 [RFC2119, RFC8174].

2. Why obsolete RFC 4345

RFC 4345 defines the "arcfour-128" and "arcfour-256" modes for Secure Shell (SSH), and is moved to Historic as RC4 is extremely weak [RFC6649, RFC7457, RFCxxxx] and there is research that is at least 5 years old that totally breaks all practical usage of RC4 [RFC6649].

3. Updates to RFC 3501

The second paragraph of [RFC3501] required that implementations of IMAP clients and servers implement a RC4 cipher suite in TLS (contradicts [RFC7465]) and recommends implementing a weak cipher suite (3DES is used in the suite). Unfortunately, at the time of writing of RFC 3501, AES cipher suites were extremely new (the first AES cipher suites were defined in RFC 3268, published in June 2002), less than 1 year old and the strongest choice they have come up with at the time was TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA.

As the document is over 14 years old, the second paragraph of Section 11.1 of [RFC3501] is replaced with the following paragraph:

"""
IMAP client and server implementations were formerly required to implement TLS_RSA_WITH_RC4_128_MD5 {TLS}, an extremely weak cipher suite [RFC6151] [RFC6649] [RFC7457] [RFCxxxx] [RFCyyyy] that TLS clients MUST NOT implement per [RFC7465]. Compatibility requirements were removed in the grounds of security, and all clients and servers SHOULD comply to [RFC7525].
"""

The TLS reference in [RFC3501] should be replaced with a reference to RFC 5246, and references to RFC 6151, RFC 6649, RFC 7457, RFC 7465, RFC xxxx and this document (as RFC yyyy) should be added.

4. Updates to RFC 4253

RFC 4253 is updated to note the deprecation of arcfour and 3des-cbc.

This document changes "OPTIONAL" to "NOT RECOMMENDED" for arcfour and

"REQUIRED" to "OPTIONAL" for 3des-cbc in the table of Section 6.3 of [RFC4253] as 3DES is weak and maintaining the requirement will compromise systems. [RFC4253] was published in 2006, 11 years ago, and states that """At some future time, it is expected that another algorithm, one with better strength, will become so prevalent and ubiquitous that the use of "3des-cbc" will be deprecated by another STANDARDS ACTION."""

The "future time" referred to by [RFC4253] is set to 2017, the "STANDARDS ACTION" is set to the publication of this document and the "algorithm" is set to the Advanced Encryption Standard (AES), as AES is ubiquitous in Kerberos implementations (see Section 11).

The last sentence of the paragraph on RC4 (called "arcfour" in [RFC4253]) in Section 6.3 of [RFC4253] should read: "Arcfour (and RC4) are extremely weak [RFC6649] [RFC7457] [RFCxxxx] [RFCyyyy] and therefore their use is NOT RECOMMENDED."

References to RFC 6649, RFC 7457, RFC xxxx and this document (the reference to this document is RFCyyyy in the above paragraph) should be added to Section 6.3 of [RFC4253].

5. Updates to RFC 6649

RFC 6649, also known as BCP 179, depreciates DES, RC4-HMAC-EXP and other weak cryptography in Kerberos. It is updated to note the deprecation of rc4-hmac and the deprecation of RC4 in all IETF protocols.

The security considerations of [RFC6649] (Section 6 of [RFC6649]) read, in their last paragraph:

"""
The security considerations of [RFC4757] continue to apply to RC4-HMAC, including the known weaknesses of RC4 and MD4, and this document does not change the Informational status of [RFC4757] for now. The main reason to not actively discourage the use of RC4-HMAC is that it is the only encryption type that interoperates with older versions of Microsoft Windows once DES and RC4-HMAC-EXP are removed. These older versions of Microsoft Windows will likely be in use until at least 2015.
"""

This is updated to note that Windows XP is without official support for 3 years (support for Windows XP ended 8 April 2014).

6. Updates to RFC 6733

Section 13.1 of [RFC6733] required that clients implement two RC4 cipher suites and a 3DES cipher suite (but recommends implementing an AES cipher suite).

RFC 6733 was published in October 2012, and all paragraphs but the last of Section 13.1 of [RFC6733] are to be replaced with:

"""
Diameter nodes were formerly required to implement insecure RC4 cipher suites and weak 3DES cipher suites. RC4 MUST NOT be used because it is prohibited by RFC 7465.

Diameter nodes MUST comply to [RFC7525].

TLS_RSA_WITH_AES_128_CBC_SHA was not chosen to be absolutely required as Diameter nodes may require all connections to use forward secrecy by only implementing cipher suites with forward secrecy. TLS_RSA_WITH_AES_128_CBC_SHA is not a forward secrecy cipher suite because all connections can be decrypted once the private RSA key is known by an attacker.
"""

7. Action to be taken

RC4 MUST NOT be used in new implementations of IETF protocols, and RC4 MUST be eliminated as fast as possible from the existing Internet infrastructure, as RC4 is insecure [RFC6649] [RFC7457] [RFCxxxx].

Vendors SHOULD take action to eradicate RC4 in all their software and systems.

New IETF protocols MUST NOT allow RC4, and new versions of existing IETF protocols MUST either not allow RC4 or recommend not to use RC4 (for example, using "NOT RECOMMENDED" or "SHOULD NOT").

8. IANA Considerations

IANA may need to take action as the status for RC4 and 3DES algorithms for Secure Shell (SSH) is changed by this document (see Section 6, that updates [RFC4253]).

9. Security Considerations

This document depreciates RC4, that is obsolete cryptography, and several attacks that render it useless have been published [RFC6649]. Refer to Section 5 of [RFCxxxx] for further security considerations.

10. Acknowledgements

[[RFC-Editor: When possible, add native names according to the conventions of RFC 7997.]]

Thanks to the following people:

* Sean Turner and Lily Chen for writing RFC 6151, that contains updated security considerations for MD5 and HMAC-MD5.

* Love Hornquist Astrand and Tom Yu for writing RFC 6649, that depreciates weak cryptographic algorithms in Kerberos.

* Yaron Sheffer, Ralph Holz and Peter Saint-Andre for writing RFC 7457, that summarises known attacks against Transport Layer Security (TLS), and RFC 7525, that provides recommendations for the use of TLS and Datagram Transport Layer Security (DTLS).

* Andrei Popov for writing RFC 7465, that prohibits RC4 cipher suites in Transport Layer Security (TLS).

* Julien Elie for sending me an email about the requirements to implement RC4 cipher suites in RFC 3501 and RFC 6733.

Refer to the acknowledgements section of RFC 6649, RFC 7457 and RFC xxxx for further acknowledgements.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC6649] Hornquist Astrand, L. and T. Yu, "Deprecate DES, RC4-HMAC-

EXP, and Other Weak Cryptographic Algorithms in Kerberos", BCP 179, RFC 6649, July 2012.

[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, May 2015.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017.

[RFCxxxx] Kaduk, B., and M. Short, "Deprecate 3DES and RC4 in Kerberos", draft-ietf-curdle-des-des-des-die-die-die-05, Work in Progress.

11.2. Informative References

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - Version 4rev1", RFC 3501, March 2003.

[RFC4253] Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, January 2006.

[RFC4757] Jaganathan, K., Zhu, L., and J. Brezak, "The RC4-HMAC Kerberos Encryption Types Used by Microsoft Windows", RFC 4757, December 2006.

[RFC6151] Turner, S., and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, March 2011.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, October 2012.

[RFC7457] Sheffer, Y., Holz, R., and P. Saint-Andre, "Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)", RFC 7457, February 2015.

[RFC7465] Popov, A., "Prohibiting RC4 Cipher Suites", RFC 7465, February 2015.

[[RFC-Editor: please replace the 'i' in my name by U+00ED and the first 'a' in the surname by U+00E2, as non-ASCII characters are allowed as per RFC 7997]]

12. Author's Address

Luis Camara

EMail: <luis.camara@live.com.pt>

Appendix A. Changelog

[[RFC-Editor: please remove this section when publishing.]]

WG draft:

03 - Style changes, removed SSL Labs paragraph in the acknowledgements section and updated RFCxxxx reference to v05. Now British English is used in all parts of the document, except quotations.

02 - Addressed Todd Short's concerns.

01 - Massive simplification: removed informational updates, removed all Pre-5378 Material, retracted all "Obsoletes:" except for RFC 4345, removed Appendix A and renamed changelog to Appendix A.

00 - Dummy update to get the draft into the curdle WG.

Individual draft:

02 - Changed title to "Deprecating RC4 in all IETF Protocols", changed the header of all pages to "Deprecating RC4 in all Protocols", updated RFC 3501 and RFC 6733, simplified the reference to draft-ietf-curdle-des-des-des-die-die-die to a simple "Work in Progress" reference and fixed typos.

01 - Explained reasons for updating RFC 7905 and added an informative reference to RFC 4757 to take away a missing reference warning.

00 - First version. [RFCxxxx] is a reference to draft-ietf-curdle-des-des-des-die-die-die. The quote in Section 11 is from version 03 of this draft (posted 2017-06-15)