Internet Engineering Task Force (IETF)
Internet-Draft
Obsoletes: 3078, 3079, 4345, 4757, 6229
Updates: 2118, 3501, 3961, 4120, 4253, 6150
Updates: 6649, 6733, 7457, 7905, xxxx
Intended Status: Best Current Practice
Expires: January 4, 2018

L. Camara
July 3, 2017

Deprecating RC4 in all IETF Protocols
draft-ietf-curdle-rc4-die-die-die-00

[[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. Documents that provide technology that can only use RC4 are obsoleted by this document, so this document obsoletes and moves to Historic RFC 3078 "Microsoft Point-to-Point Encryption (MPPE) Protocol" (only supports RC4, RFC 3079 that is also part of that protocol is also obsoleted), RFC 4345 "Improved Arcfour Modes for the Secure Shell (SSH) Transport Layer Protocol" (note Arcfour and RC4 are synonymous), RFC 4757 "The RC4-HMAC Kerberos Encryption Types Used by Microsoft Windows" (only supports RC4) and RFC 6229 "Test Vectors for the Stream Cipher RC4" (provides test vectors for historic cryptography). RFC 2118, RFC 3501, RFC 3961, RFC 4120, RFC 4253, RFC 6150, RFC 6649, RFC 6733, RFC 7457, RFC 7905 and RFC xxxx are updated to note the deprecation of RC4 in all IETF protocols. (Please do not confuse RFC 4757 with RFC 7457.)

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 January 4, 2018.

Table of Contents

1. Introduction

RC4 is extremely weak [RFC6649, RFC7457, RFCxxxx] and this document deprecates its use in all IETF protocols, including Kerberos and Secure Shell (SSH). The reasons for obsoleting RFC 3078, RFC 3079, RFC 4345 and RFC 4757 and moving them to Historic are discussed in Section 2. The updates to RFC 2118, RFC 3501, RFC 3961, RFC 4120, RFC 4253, RFC 6150, RFC 6649, RFC 6733, RFC 7457, RFC 7905 and RFC xxxx and the reasons for doing them are specified in sections 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 and 14, respectively. The status of

the updated RFCs as of the writing of this document is available in Appendix A.

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 those RFCs and move them to Historic

RFC 3078 is no longer used by supported Microsoft Windows versions and is moved to Historic and obsoleted by this document as it only supports RC4 for encryption. RFC 2118 is updated to note the moving of RFC 3078 (that updated RFC 2118) to Historic and its obsoleting. RFC 3079, that is effectively part of RFC 3078, is also moved to Historic as it only supports RC4 for encryption.

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].

RFC 4757 is obsoleted and moved to Historic as it is no longer used by supported Microsoft Windows versions (support for Windows XP ended 8 April 2014, any unofficial support for officially unsupported Microsoft Windows versions will certainly remove RC4) and specifies RC4-HMAC as used by Microsoft Windows in Kerberos, that should have been obsoleted, not updated, by RFC 6649. RFC xxxx also obsoletes RFC 4757. Additionally, MD4 is extremely weak and not one-way [RFC6150] and this is another reason to move RFC 4757 to Historic, as well as the myriads of other reasons specified

in [RFC6150].

RFC 6229 provides test vectors for RC4 and is obsoleted and moved to Historic by this document as RC4 is deprecated in all IETF protocols.

3. Updates to RFC 2118

RFC 2118 is updated to note the obsoleting of RFC 3078 and the moving of RFC 3078 to Historic (see Section 2).

4. Updates to RFC 3501

In Section 11.1 of [RFC3501], it is stated that:

"""
IMAP client and server implementations MUST implement the TLS_RSA_WITH_RC4_128_MD5 {TLS} cipher suite, and SHOULD implement the TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA {TLS} cipher suite. This is important as it assures that any two compliant implementations can be

configured to interoperate. All other cipher suites are OPTIONAL. Note that this is a change from section 2.1 of {IMAP_TLS}.
"""

[[References were replaced with curly braces to avoid nits. When publishing, revert back to references.]]

The above 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 (DSA is not recommended by some sources and 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 above paragraph 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 implement TLS 1.2 {TLS} and the TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 {TLS} cipher suite.
"""

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.

5. Updates to RFC 3961

RFC 3961 is updated to note the deprecation of rc4-hmac and rc4-hmac-exp (referred to in Section 8 of [RFC3961]). rc4-hmac is NOT RECOMMENDED by [RFCxxxx] and rc4-hmac-exp is NOT RECOMMENDED by [RFC6649].

6. Updates to RFC 4120

RFC 4120 is updated to note the deprecation of rc4-hmac and rc4-hmac-exp.

7. 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 paragraph on RC4 (called "arcfour" in [RFC4253]) in Section 6.3 of [RFC4253] currently reads:
"""
The "arcfour" cipher is the Arcfour stream cipher with 128-bit keys.

The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should be used with caution.
"""

It should read:
"""
The "arcfour" cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. 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].

8. Updates to RFC 6150

RFC 6150 moves MD4 to Historic. Note the RFC contains a typo: "MD2" should be "MD4". RFC 6150 references RFC 4757, obsoleted by this document, as using MD4. The expression "with the one exception of Microsoft's use of MD4 as part of RC4-HMAC in Windows,", as well as all expressions indicating algorithms using RC4 are a problem to the deprecation of MD4, should be removed from Section 4 of [RFC6150].

9. Updates to RFC 6649

RFC 6649, also known as BCP 179, deprecates 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).

An important quote from [RFC6649] (Section 6 of [RFC6649]):
"""
Removing support for single DES improves security because DES is considered to be insecure. RC4-HMAC-EXP has a similarly inadequate key size, so removing support for it also improves security.
"""

10. Updates to RFC 6733

Section 13.1. of [RFC6733] currently reads:
"""
Diameter nodes MUST be able to negotiate the following TLS/TCP and DTLS/SCTP cipher suites:

```
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

Diameter nodes SHOULD be able to negotiate the following TLS/TCP and DTLS/SCTP cipher suite:

```
TLS_RSA_WITH_AES_128_CBC_SHA
```

Note that it is quite possible that support for the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite will be REQUIRED at some future date. Diameter nodes MAY negotiate other TLS/TCP and DTLS/SCTP cipher suites.
"""

The above paragraphs 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 the above paragraphs 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 support at least one of the following cipher suites:

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
```

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.
"""

Several choices were given because of patent concerns with Elliptic Curve Cryptography (ECC) and problems of older implementations with ECC and GCM cipher suites.

11. Updates to RFC 7457

RFC 7457, an Informational RFC describing attacks against Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), is updated to note the deprecation of RC4 in all IETF protocols.

12. Updates to RFC 7465

RFC 7465 prohibits RC4 cipher suites in Transport Layer Security (TLS) and is updated to note the deprecation of RC4 in all IETF protocols.

13. Updates to RFC 7905

RFC 7905, describing the ChaCha20-Poly1305 stream cipher to replace RC4 in Transport Layer Security (TLS), is updated to note the deprecation of RC4 in all IETF protocols, including TLS. [RFC7465],

that prohibited RC4 cipher suites, did not update RFC 7905, so this document will do so.

14. Updates to RFC xxxx

RFC xxxx deprecates 3DES and RC4 in Kerberos, obsoletes RFC 4757 and updates RFC 3961, and is updated by this document to note the moving of RC4 RFCs (RFC 4345 and RFC 6229) and Microsoft technology dependent on RC4 (RFC 3078 and RFC 4757).

An important quote from [RFCxxxx] (Section 5.4 of [RFCxxxx]):
"""
Fortuntately, modern (i.e., supported) Kerberos implementations support a secure alternative to RC4, in the form of AES. Windows has supported AES since 2007-2008 with the release of Windows Vista and Server 2008, respectively; MIT Kerberos [MITKRB5] has fully supported AES (including the GSSAPI mechanism) since 2004 with the release of version 1.3.2; Heimdal [HEIMDAL] has fully supported AES since 2005 with the release of version 0.7. Though there may still be issues running ten-year-old unsupported software in mixed environments with new software, issues of that sort seem unlikely to be unique to Kerberos, and the aministrators of such environments are expected to be capable of devising workarounds.
"""
(note the quote contains typos: "Fortuntately" and "aministrators")

15. 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 extremely weak [RFC6649, RFC7457, RFCxxxx]. New RFCs MAY use the phrase "RC4 is extremely weak [RFC6649, RFC7457, RFCxxxx]" with references to RFC 6649, RFC 7457 and RFC xxxx. Whether the references to these documents is normative or informative is determined by BCP 9 and BCP 97, whose relevant documents for this purpose are RFC 2026, RFC 3967, RFC 4897, RFC 6410 and RFC 8067.

Microsoft Corporation SHOULD take action to eradicate RC4 in all its 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").

16. 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]).

17. Security Considerations

This document deprecates 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.

18. Acknowledgements

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

Thanks to the following people for writing reference material:

* 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 deprecates 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).

* 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.

Also thanks to SSL Labs for capping server grades to B (RC4 only used with older protocols) and C (RC4 used with modern protocols) when servers support RC4, and flagging cipher suites and clients using RC4 with a red colour (for INSECURE and RC4). You can test any server at <https://www.ssllabs.com/ssltest/>.

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

19. References

19.1. 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.

[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-03, Work in Progress.

19.2. Informative References

[HEIMDAL] Heimdal Project, "Heimdal Kerberos Implementation", April 2017, <https://www.h5l.org/>.

[MITKRB5] MIT, "MIT Kerberos Implementation", March 2017, <https://web.mit.edu/kerberos/>.

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

[RFC3961] Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5", RFC 3961, February 2005.

[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 2606.

[RFC6150] Turner, S., and L. Chen, "MD4 to Historic Status", RFC 6150, March 2011.

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

[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., "Deprecating RC4 Cipher Suites", RFC 7465, February 2015.

[SCHNEIER] Schneier, B., "Applied Cryptography Second Edition: protocols algorithms and source in code in C", John Wiley and Sons, New York, NY, 1996.

[[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]]

20. Author's Address

Luis Camara

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

Appendix A. Status of Updated Documents as of 2017-06-24

[[RFC-Editor: Please replace with updated data when publishing as RFC and replace "2017-06-24" by the date of publishing.
Leave the table below in a page of its own.]]

RFC ####	Status	Updated by
RFC 2118	Informational	RFC 3078
RFC 3501	Proposed Standard	RFC 4466, RFC 4469, RFC 4551, RFC 5032, RFC 5182, RFC 5738, RFC 6186, RFC 6858, RFC 7817
RFC 3961	Proposed Standard	RFC xxxx
RFC 4120	Proposed Standard	RFC 4537, RFC 5021, RFC 5896, RFC 6111, RFC 6112, RFC 6113, RFC 6649, RFC 6806, RFC 7751, RFC 8062, RFC 8129
RFC 4253	Proposed Standard	RFC 6668
RFC 6150	Informational	

RFC 6649	Best Current Practice (BCP 179)	
RFC 6733	Proposed Standard	RFC 7075
RFC 7457	Informational	
RFC 7465	Proposed Standard	
RFC 7905	Proposed Standard	
RFC xxxx	Best Current Practice	This draft is [RFCxxxx]

Appendix B. Changelog

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

WG draft (draft-ietf-curdle-rc4-die-die-die):

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

Individual draft (draft-luis140219-curdle-rc4-die-die-die):

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)