Internet Engineering Task Force (IETF)
Request for Comments: 8758
BCP: 227
Updates: 4253
Category: Best Current Practice
ISSN: 2070-1721

L. Velvindron
cyberstorm.mu

April 2020

Deprecating RC4 in Secure Shell (SSH)

Abstract

This document deprecates RC4 in Secure Shell (SSH). Therefore, this document formally moves RFC 4345 to Historic status.

Status of This Memo

This memo documents an Internet Best Current Practice.

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 BCPs 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/rfc8758.

Table of Contents

1. Introduction

The usage of RC4 suites (also designated as "arcfour") for SSH is specified in [RFC4253] and [RFC4345]. [RFC4253] specifies the allocation of the "arcfour" cipher for SSH. [RFC4345] specifies and

allocates the "arcfour128" and "arcfour256" ciphers for SSH. RC4 encryption has known weaknesses [RFC7465] [RFC8429]; therefore, this document starts the deprecation process for their use in Secure Shell (SSH) [RFC4253]. Accordingly, [RFC4253] is updated to note the deprecation of the RC4 ciphers, and [RFC4345] is moved to Historic status, as all ciphers it specifies MUST NOT be used.

1.1. 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.

2. Updates to RFC 4253

[RFC4253] is updated to prohibit arcfour's use in SSH. [RFC4253], Section 6.3 allocates the "arcfour" cipher by defining a list of defined ciphers in which the "arcfour" cipher appears as optional, as shown in Table 1.

arcfour	OPTIONAL	the ARCFOUR stream cipher with a 128-bit key

Table 1

This document updates the status of the "arcfour" ciphers in the list found in [RFC4253], Section 6.3 by moving it from OPTIONAL to MUST NOT.

arcfour	MUST NOT	the ARCFOUR stream cipher with a 128-bit key

Table 2

[RFC4253] defines the "arcfour" ciphers with the following text:

> 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.

This document updates [RFC4253], Section 6.3 by replacing the text above with the following text:

> The "arcfour" cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has known weaknesses [RFC7465] [RFC8429] and MUST NOT be used.

3. IANA Considerations

The IANA has updated the "Encryption Algorithm Names" subregistry in the "Secure Shell (SSH) Protocol Parameters" registry [IANA]. The registration procedure is IETF review, which is achieved by this document. The registry has been updated as follows:

Encryption Algorithm Name	Reference	Note
arcfour	RFC 8758	HISTORIC

arcfour128	RFC 8758	HISTORIC
arcfour256	RFC 8758	HISTORIC

Table 3

4. Security Considerations

This document only prohibits the use of RC4 in SSH; it introduces no new security considerations.

5. References

5.1. 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>.

5.2. Informative References

[IANA] "Secure Shell (SSH) Protocol Parameters", <https://www.iana.org/assignments/ssh-parameters>.

[RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, DOI 10.17487/RFC4253, January 2006, <https://www.rfc-editor.org/info/rfc4253>.

[RFC4345] Harris, B., "Improved Arcfour Modes for the Secure Shell (SSH) Transport Layer Protocol", RFC 4345, DOI 10.17487/RFC4345, January 2006, <https://www.rfc-editor.org/info/rfc4345>.

[RFC7465] Popov, A., "Prohibiting RC4 Cipher Suites", RFC 7465, DOI 10.17487/RFC7465, February 2015, <https://www.rfc-editor.org/info/rfc7465>.

[RFC8429] Kaduk, B. and M. Short, "Deprecate Triple-DES (3DES) and RC4 in Kerberos", BCP 218, RFC 8429, DOI 10.17487/RFC8429, October 2018, <https://www.rfc-editor.org/info/rfc8429>.

[SCHNEIER] Schneier, B., "Applied Cryptography Second Edition: Protocols, Algorithms, and Source in Code in C", John Wiley and Sons New York, NY, 1996.

Acknowledgements

The author would like to thank Eric Rescorla, Daniel Migault, and Rich Salz.

Author’s Address

Loganaden Velvindron
cyberstorm.mu
Mauritius

Email: logan@cyberstorm.mu