

Internet Engineering Task Force
Internet-Draft
Obsoletes: [4345](#) (if approved)
Intended status: Best Current Practice
Expires: July 20, 2019

L. Camara
L. Velvindron
cyberstorm.mu
January 16, 2019

**Deprecating RC4 in Secure Shell (SSH)
draft-ietf-curdle-rc4-die-die-die-15**

Abstract

This document deprecates RC4 in Secure Shell (SSH). Therefore, this document formally obsoletes and moves to Historic [RFC4345](#).

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 July 20, 2019.

Copyright Notice

Copyright (c) 2019 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
1.1.	Requirements Language	2
2.	Updates to RFC 4253	2
3.	IANA Considerations	3
4.	Acknowledgements	3
5.	Security Considerations	3
6.	References	4
6.1.	Normative References	4
6.2.	Informative References	4
	Authors' Addresses	4

[1.](#) Introduction

The usage of RC4 suites (also designated as arcfour) for SSH are specified in [[RFC4253](#)] and [[RFC4345](#)]. [[RFC4253](#)] specifies the allocation of the "arcfour" cipher for SSH. [[RFC4345](#)] specifies and allocates the "arcfour-128" and "arcfour-256" ciphers for SSH. RC4 encryption has known weaknesses [[RFC7465](#)] [[I-D.ietf-curdle-des-des-des-die-die-die](#)], and the deprecation process should be begun 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 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", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

[2.](#) Updates to [RFC 4253](#)

[[RFC4253](#)] is updated to prohibit arcfour's use in SSH. [[RFC4253](#)] allocates the "arcfour" cipher in [Section 6.3](#) by defining a list of defined ciphers where the "arcfour" cipher appears as optional as mentioned below:

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

The current document updates the status of the "arcfour" ciphers in the list of [[RFC4253](#)] [Section 6.3](#) by moving it from OPTIONAL to MUST NOT.


```

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

```

[RFC4253] defines the "arcfour" ciphers with the text mentioned below:

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 problems with weak keys, and should be used with caution.

The current 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](#)] [[I-D.ietf-curdle-des-des-des-die-die-die](#)], and MUST NOT be used.

3. IANA Considerations

The IANA is requested to update the Encryption Algorithm Name Registry of the Secure Shell (SSH) Protocol Parameters [[IANA](#)]. The Registration procedure is IETF Review which is achieved by this document. The registry should be updated as follows:

```

+-----+-----+-----+-----+
| Encryption | Algorithm Name | Reference | Note |
+-----+-----+-----+-----+
| arcfour    | [RFC-TBD]      |           |      |
| arcfour128 | [RFC-TBD]      |           |      |
| arcfour256 | [RFC-TBD]      |           |      |
+-----+-----+-----+-----+

```

Where TBD is the RFC number assigned to the document.

4. Acknowledgements

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

5. Security Considerations

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

6. References

6.1. 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>>.

6.2. Informative References

- [I-D.ietf-curdle-des-des-des-die-die-die] Kaduk, B. and M. Short, "Deprecate 3DES and RC4 in Kerberos", [draft-ietf-curdle-des-des-des-die-die-die-05](#) (work in progress), September 2017.
- [IANA] "Secure Shell (SSH) Protocol Parameters: Encryption Algorithm Names", <<https://www.iana.org/assignments/ssh-parameters/ssh-parameters.xhtml#ssh-parameters-17>>.
- [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>>.
- [SCHNEIER] Schneier, B., "Applied Cryptography Second Edition: protocols algorithms and source in code in C", , 1996, <SCHNEIER>.

Authors' Addresses

Luis Camara

Email: luis.camara@live.com.pt

Loganaden Velvindron
cyberstorm.mu
Mauritius

Email: loganaden@gmail.com