Internet Engineering Task Force (IETF)
Internet-Draft
Obsoletes: 4345 (if approved)
Updates: 4253 (if approved)
Intended Status: Best Current Practice
Expires: July 22, 2018

L. Camara
L.Velvindron

July 22, 2018

Deprecating RC4 in Secure Shell (SSH)
draft-ietf-curdle-rc4-die-die-die-07

[[RFC-Editor: please replace the second character of my surname by U+00E2 when publishing as RFC in the header and in all pages.]]

Abstract

This document deprecates RC4 in Secure Shell (SSH). Therefore, this document updates RFC 4253, and moves to Historic RFC 4345.

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 July 30, 2018.

Copyright Notice

Internet-Draft Deprecating RC4 in Secure Shell January 2018

Table of Contents

1. Introduction

The usage of RC4 suites (also designated as arcfour) for SSH are specified in [RFC 4253] and [RFC 4345]. [RFC 4253] specifies the allocation of the "arcfour" cipher for SSH. RFC 4345 specifies and allocates the the "arcfour-128" and "arcfour-256" ciphers for SSH.

RC4 encryption is steadily weakening in cryptographic strength [RFC7457] [draft-ietf-curdle-des-des-des-die-die-die-05] and the deprecation process should be begun for their use in SSH.

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] when, and only when, they appear in all capitals, as shown here.

2. Why obsolete and move to Historic RFC 4345

RFC 4345 defines the "arcfour-128" and "arcfour-256" modes for SSH, and is obsoleted and moved to Historic as RC4 is broken [RFC7457]. The modes defined by RFC 4345 MUST NOT be used.

3. Updates to RFC 4253

RFC 4253 is updated to prohibit arcfour's use in SSH.

The last sentence of the paragraph on RC4 (called "arcfour" in [RFC4253]) in Section 6.3 of [RFC4253] should read: "Arcfour (also known as RC4) is broken [RFC7457] and therefore it MUST NOT be used."

An informative reference to RFC 7457 is to be added to [RFC4253].

4. 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 3, that updates [RFC4253]).

5. Security Considerations

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

6. Acknowledgements

Thanks to the numerous authors which have shown the weaknesses of RC4 throughout the years, and to the several people which have commented on the CURDLE mailing list about this document.

7. References

7.1. Normative References

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

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

7.2. Informative References

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

[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.

[[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]]

8. Author's Address

Luis Camara

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

Loganaden Velvindron

EMail: <loganaden@gmail.com>