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.

Copyright Notice

Copyright (c) 2020 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
   1.1. Requirements Language
2. Updates to RFC 4253
3. IANA Considerations
4. Security Considerations
5. References
   5.1. Normative References
   5.2. Informative References
Acknowledgements
Author’s Address

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.

<table>
<thead>
<tr>
<th>arcfour</th>
<th>OPTIONAL</th>
<th>the ARCFOUR stream cipher with a 128-bit key</th>
</tr>
</thead>
</table>

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.

<table>
<thead>
<tr>
<th>arcfour</th>
<th>MUST NOT</th>
<th>the ARCFOUR stream cipher with a 128-bit key</th>
</tr>
</thead>
</table>

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:

<table>
<thead>
<tr>
<th>Encryption Algorithm Name</th>
<th>Reference</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>arcfour</td>
<td>RFC 8758</td>
<td>HISTORIC</td>
</tr>
<tr>
<td>arcfour128</td>
<td>RFC 8758</td>
<td>HISTORIC</td>
</tr>
</tbody>
</table>
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


5.2. Informative References


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