Internet Engineering Task Force (IETF)
Request for Comments: 8270
Updates: 4419
Category: Standards Track
ISSN: 2070-1721

L. Velvindron
Hackers.mu
M. Baushke
Juniper Networks, Inc.

December 2017

Increase the Secure Shell Minimum Recommended Diffie-Hellman Modulus Size to 2048 Bits

Abstract

The Diffie-Hellman (DH) Group Exchange for the Secure Shell (SSH) transport-layer protocol specifies that servers and clients should support groups with a minimum modulus group size of 1024 bits. Recent security research has shown that the minimum value of 1024 bits is insufficient to protect against state-sponsored actors and any organization with enough computing resources. This RFC updates RFC 4419, which allowed for DH moduli less than 2048 bits; now, 2048 bits is the minimum acceptable group size.

Status of This Memo

This is an Internet Standards Track document.

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 Internet Standards 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/rfc8270.

Table of Contents

1. Introduction

[RFC4419] specifies a recommended minimum DH modulus group size of 1024 bits. It also suggests that in all cases, the size of the group needs to be at least 1024 bits. This document updates [RFC4419] so that the minimum recommended size is 2048 bits. This recommendation is based on recent research [LOGJAM] on DH group weaknesses. This minimum DH group size may need to be increased to 3072 for forward-looking users.

2. 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.

3. 2048-Bit DH Group

Recent research [LOGJAM] strongly suggests that DH groups that are 1024 bits can be broken by state-sponsored actors and any organization with enough computing resources. The authors show how they are able to break 768-bit DH groups and extrapolate the attack to 1024-bit DH groups. In their analysis, they show that breaking 1024 bits can be done with sufficient computing resources. This document provides the following recommendation: SSH servers and SSH clients SHOULD support groups with a minimum acceptable group size of 2048 bits for the "min" value of the SSH_MSG_KEY_DH_GEX_REQUEST client message given in [RFC4419]. Further, SSH clients SHOULD be able to send a value of 3072 bits for the preferred acceptable group size "n" in the SSH_MSG_KEY_DH_GEX_REQUEST message.

[RFC4419] specifies a recommended minimum size of 1024 bits for k, which is the modulus length of the DH group. It also suggests that, in all cases, the size of the group needs be at least 1024 bits. This document updates [RFC4419] as described below:

- Section 3, paragraph 9:
  Servers and clients SHOULD support groups with a modulus length of k bits where 2048 <= k <= 8192. The recommended minimum values for min and max are 2048 and 8192, respectively. Setting k to 3072 SHOULD be possible, as the need may arise in the coming years.

- Section 3, paragraph 11:
  In all cases, the size of the group SHOULD be at least 2048 bits. Setting the group size to 3072 SHOULD be possible, as the need may arise in the coming years.

4. Interoperability

This document keeps the following requirement from [RFC4419]:

> The server should return the smallest group it knows that is larger than the size the client requested. If the server does not know a group that is larger than the client request, then it SHOULD return the largest group it knows.

Also, it updates the subsequent sentence as follows:

> In all cases, the size of the returned group SHOULD be at least 2048 bits. Setting the group size to 3072 SHOULD be possible, as the need may arise in the coming years.

5. Security Considerations

This document discusses security issues of DH groups that are 1024 bits in size, and formally updates the minimum size of DH groups to be 2048 bits. A hostile or "owned" SSH server implementation could potentially use backdoored DH primes using the methods described in [Backdoor-DH] to provide the g and p values to be used. Or, it could just send the calculated secret through a covert channel of some sort to a passive listener.

A malicious client could cause a Denial of Service by intentionally making multiple connections that are less than 2048 bits in size. Therefore, operating systems SHOULD NOT log DH groups that are less than 2048 bits in size, as it would create an additional attack surface.

6. IANA Considerations

This document does not require any IANA actions.

7. References

7.1. 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>.

[RFC4419] Friedl, M., Provos, N., and W. Simpson, "Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol", RFC 4419, DOI 10.17487/RFC4419, March 2006, <https://www.rfc-editor.org/info/rfc4419>.

[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>.

7.2. Informative References

[Backdoor-DH] Wong, D., "How to Backdoor Diffie-Hellman", Cryptology ePrint Archive Report 2016/644, June 2016, <http://eprint.iacr.org/2016/644.pdf>.

[LOGJAM] Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J., Heninger, N., Springall, D., Thome, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Beguelin, S., and P. Zimmermann, "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice", ACM Conference on Computer and Communications Security (CCS) 2015, DOI 10.1145/2810103.2813707, 2015, <https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf>.

Authors' Addresses

Loganaden Velvindron
Hackers.mu
88, Avenue De Plevitz
Roches Brunes
Mauritius

Phone: +230 59762817
Email: logan@hackers.mu

Mark D. Baushke
Juniper Networks, Inc.

Email: mdb@juniper.net