Increase SSH minimum recommended DH modulus size to 2048 bits
draft-ietf-curdle-ssh-dh-group-exchange-03

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 modulus length of k bits, where the recommended
   minumum value is 1024 bits. Recent security research has shown that
   a minimum value of 1024 bits is insufficient against state-sponsored
   actors. As such, this document formally updates the specification
   such that the minimum recommended value for k is 2048 bits and the
   group size is 2048 bits at minimum. This RFC updates RFC4419 which
   allowed for DH moduli less than 2048 bits.

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 December 22, 2017.

Copyright Notice

1. Introduction

[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] so that the minimum recommended size be 2048 bits. This recommendation is based on recent research [LOGJAM] on DH Group weaknesses.

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. 2048 bits DH Group

Recent research [LOGJAM] strongly suggests that DH groups that are 1024 bits can be broken by state actors, and possibly an organization with enough computing resources. The authors show how they are able to break 768 bits DH group and extrapolate the attack to 1024 bits DH groups. In their analysis, they show that breaking 1024 bits can be done with enough computing resources. This document provides the following recommendation: SSH Servers and SSH clients SHOULD support groups with a modulus length of k bits where 2048 <= k <= 8192.

[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. This document also
updates [RFC 4419] Section 3 Paragraph 11 as follows: In all cases,
the size of the group SHOULD be at least 2048 bits.

3. Interoperability

As state in [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.

4. 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" Secure Shell server
implementation could potentially use Backdoored Diffie-Hellman primes
using the methods described in [Backdoor-DH] to provide the g,p
values to be used. Or, they could just send the calculated secret
through a covert channel of some sort to a passive listener.

5. IANA Considerations

This document contains no considerations for IANA.

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,
           <http://www.rfc-editor.org/info/rfc2119>.

6.2. 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, 2015, <https://weakdh.org/imperfect-forward-
               secrecy-ccs15.pdf>.

   [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,
               <http://www.rfc-editor.org/info/rfc4419>.

Authors' Addresses

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

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

   Mark D. Baushke
   Juniper Networks, Inc.

   Email: mdb@juniper.net