Internet Engineering Task Force
Internet-Draft
Updates: 5246 7525 (if approved)
Intended status: Standards Track
Expires: November 10, 2019

L. Velvindron
cyberstorm.mu
K. Moriarty
Dell EMC

May 9, 2019

Deprecating MD5 and SHA1 in TLS 1.2
draft-lvelvindron-tls-md5-sha1-deprecate-03

Abstract

The MD5 and SHA1 hashing algorithms are steadily weakening in strength and their deprecation process should begin for their use in TLS 1.2 digital signatures.

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 November 10, 2019.

Copyright Notice

Table of Contents

1. Introduction

The usage of MD5 and SHA1 for TLS 1.2 is specified RFC 5246 [RFC5246]. MD5 and SHA-1 have been proven to be insecure, subject to collision attacks. RFC 6151 [RFC6151] details the security considerations, including collision attacks for MD5, published in 2011. MD5 has been deprecated by NIST and is no longer mentioned in publications such as [NISTSP800-131A-R2]. NIST formally deprecated use of SHA-1 in 2011 [NISTSP800-131A-R2] and disallowed its use for digital signatures at the end of 2013, based on both the Wang, et. al, attack and the potential for brute-force attack. Further, in 2017, researchers from Google and CWI Amsterdam [SHA-1-Collision] proved SHA-1 collision attacks were practical. This document updates RFC 5246 [RFC5246] and RFC7525 [RFC7525] in such as way that MD5 and SHA1 MUST NOT be used for digital signatures.

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. Signature Algorithms

Clients SHOULD NOT include md5 and SHA-1 in signature_algorithms extension. If a client does not send a signature_algorithms

extension, then the server MUST abort the handshake and send a handshake_failure alert.

3. Certificate Requests

Servers SHOULD NOT include md5 and SHA-1 in CertificateRequest message.

4. Server Key Exchange

Servers MUST NOT include md5 and SHA-1 in ServerKeyExchange message. If client does receive a MD5 or SHA-1 signature in the ServerKeyExchange message it MUST abort the connection with handshake_failure or insufficient_security alert.

5. Certificate Verify

Clients MUST NOT include md5 and SHA-1 in CertificateVerify message.

6. Updates to RFC5246

OLD:

In Section 7.4.1.4.1: the text should be revised from " enum { none(0), md5(1), sha1(2), sha224(3), sha256(4), sha384(5), sha512(6), (255) } HashAlgorithm;"

NEW:

enum { none(0), sha224(3), sha256(4), sha384(5), sha512(6), (255) } HashAlgorithm;

OLD:

In Section 7.4.1.4.1: the text should be revised from " Note: this is a change from TLS 1.1 where there are no explicit rules, but as a practical matter one can assume that the peer supports MD5 and SHA-1."

NEW:

"Note: This is a change from TLS 1.1 where there are no explicit rules, but as a practical matter one can assume that the peer supports SHA-256."

7. Updates to RFC7525

RFC7525 [RFC7525], Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) recommends use of SHA-256 as a minimum requirement. This update moves the minimum recommendation to use stronger language deprecating

use of both SHA-1 and MD5. The prior text did not explicitly include MD5 and this text adds it to ensure it is understood as having been deprecated.

Section 4.3:

OLD:

When using RSA, servers SHOULD authenticate using certificates with at least a 2048-bit modulus for the public key. In addition, the use of the SHA-256 hash algorithm is RECOMMENDED (see [CAB-Baseline] for more details). Clients SHOULD indicate to servers that they request SHA-256, by using the "Signature Algorithms" extension defined in TLS 1.2.

NEW:

When using RSA, servers SHOULD authenticate using certificates with at least a 2048-bit modulus for the public key. In addition, the use of the SHA-256 hash algorithm is RECOMMENDED, SHA-1 or MD5 MUST not be used (see [CAB-Baseline] for more details). Clients SHOULD indicate to servers that they request SHA-256, by using the "Signature Algorithms" extension defined in TLS 1.2.

8. Security Considerations

Concerns with TLS 1.2 implementations falling back to SHA-1 is an issue. This draft updates the TLS 1.2 specification to deprecate support for MD5 and SHA-1 for digital signatures.

9. Acknowledgement

The authors would like to thank Hubert Kario for his help in writing the initial draft.

10. References

10.1. 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>.

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <https://www.rfc-editor.org/info/rfc7525>.

10.2. Informative References

[CAB-Baseline] CA/Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Version 1.1.6", 2013, <https://www.cabforum.org/documents.html>.

[NISTSP800-131A-R2] Barker, E. and A. Roginsky, "Transitioning the Use of Cryptographic Algorithms and Key Lengths", March 2019, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008,

<https://www.rfc-editor.org/info/rfc5246>.

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, DOI 10.17487/RFC6151, March 2011, <https://www.rfc-editor.org/info/rfc6151>.

[SHA-1-Collision] Stevens, M., Bursztein, E., Karpman, P., Albertini, A., and Y. Markov, "The first collision for full SHA-1", March 2019, <http://shattered.io/static/shattered.pdf>.

Authors' Addresses

Loganaden Velvindron
cyberstorm.mu
Rose Hill
MU

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

Kathleen Moriarty
Dell EMC