Search RFCs

number, title, keyword, or author surname

Advanced Search

RFC Editor

BCP 195

Cite this BCP: TXT | XML

BCP 195 contains the following RFCs:

Number	Files	Title	Authors	Date	More Info	Status
RFC 8996, BCP 195		**Deprecating TLS 1.0 and TLS 1.1**	K. Moriarty, S. Farrell	March 2021	Obsoletes RFC 5469, RFC 7507, Updates RFC 3261, RFC 3329, RFC 3436, RFC 3470, RFC 3501, RFC 3552, RFC 3568, RFC 3656, RFC 3749, RFC 3767, RFC 3856, RFC 3871, RFC 3887, RFC 3903, RFC 3943, RFC 3983, RFC 4097, RFC 4111, RFC 4162, RFC 4168, RFC 4217, RFC 4235,	Best Current Practice

RFC 4261,
RFC 4279,
RFC 4497,
RFC 4513,
RFC 4531,
RFC 4540,
RFC 4582,
RFC 4616,
RFC 4642,
RFC 4680,
RFC 4681,
RFC 4712,
RFC 4732,
RFC 4743,
RFC 4744,
RFC 4785,
RFC 4791,
RFC 4823,
RFC 4851,
RFC 4964,
RFC 4975,
RFC 4976,
RFC 4992,
RFC 5018,
RFC 5019,
RFC 5023,
RFC 5024,
RFC 5049,
RFC 5054,
RFC 5091,
RFC 5158,
RFC 5216,
RFC 5238,
RFC 5263,
RFC 5281,
RFC 5364,
RFC 5415,
RFC 5422,
RFC 5456,
RFC 5734,
RFC 5878,
RFC 5953,
RFC 6012,
RFC 6042,
RFC 6083,
RFC 6084,
RFC 6176,
RFC 6347,
RFC 6353,
RFC 6367,
RFC 6460,
RFC 6614,
RFC 6739,
RFC 6749,
RFC 6750,
RFC 7030,
RFC 7465,
RFC 7525,

				RFC 7562, RFC 7568, RFC 8261, RFC 8422, Errata	
RFC 9325, BCP 195	**Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)**	Y. Sheffer, P. Saint-Andre, T. Fossati	November 2022	Obsoletes RFC 7525, Updates RFC 5288, RFC 6066	Best Current Practice

Abstract of RFC 8996

This document formally deprecates Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346). Accordingly, those documents have been moved to Historic status. These versions lack support for current and recommended cryptographic algorithms and mechanisms, and various government and industry profiles of applications using TLS now mandate avoiding these old TLS versions. TLS version 1.2 became the recommended version for IETF protocols in 2008 (subsequently being obsoleted by TLS version 1.3 in 2018), providing sufficient time to transition away from older versions. Removing support for older versions from implementations reduces the attack surface, reduces opportunity for misconfiguration, and streamlines library and product maintenance.

This document also deprecates Datagram TLS (DTLS) version 1.0 (RFC 4347) but not DTLS version 1.2, and there is no DTLS version 1.1.

This document updates many RFCs that normatively refer to TLS version 1.0 or TLS version 1.1, as described herein. This document also updates the best practices for TLS usage in RFC 7525; hence, it is part of BCP 195.

Abstract of RFC 9325

Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) are used to protect data exchanged over a wide range of application protocols and can also form the basis for secure transport protocols. Over the years, the industry has witnessed several serious attacks on TLS and DTLS, including attacks on the most commonly used cipher suites and their modes of operation. This document provides the latest recommendations for ensuring the security of deployed services that use TLS and DTLS. These recommendations are applicable to the majority of use cases.

RFC 7525, an earlier version of the TLS recommendations, was published when the industry was transitioning to TLS 1.2. Years later, this transition is largely complete, and TLS 1.3 is widely available. This

document updates the guidance given the new environment and obsoletes RFC 7525. In addition, this document updates RFCs 5288 and 6066 in view of recent attacks.

For the definition of **Status**, see RFC 2026.

For the definition of **Stream**, see RFC 8729.
