Análise das versões do TLS para o Python (VERSÃO PÚBLICA)

Sumário

1.TLS

TLS é o acrônimo de *Transport Layer Security* (Segurança em Camada de Transporte), um protocolo publicado em 1999 na RFC 2246. O objetivo principal do protocolo TLS é fornecer privacidade e integridade de dados entre dois aplicativos em comunicação. O protocolo é composto por duas camadas: o protocolo de registro TLS e o protocolo de handshake TLS. No nível mais baixo, sobreposto a algum protocolo de transporte confiável (por exemplo, TCP[TCP]), está o protocolo de registro TLS. A Figura 1 mostra como o TLS é implementado na camada de Sessão do modelo Open systems interconnection (OSI)[1].

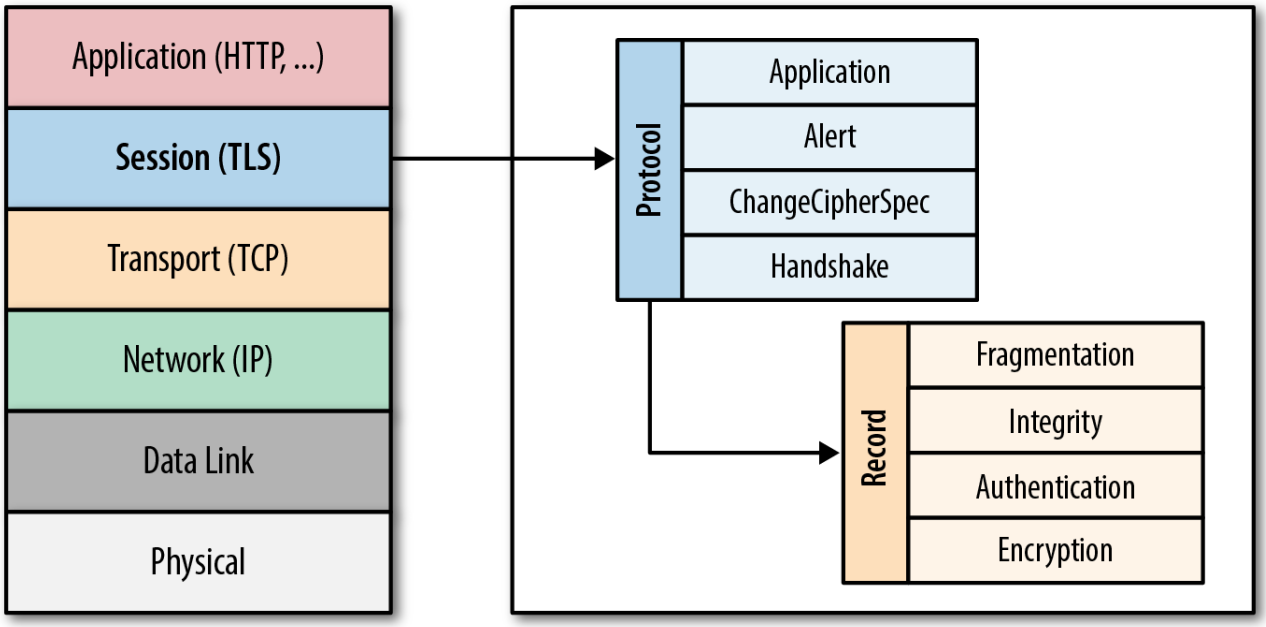

Figura 1: Arquitetura do protocolo Transport Layer Security (TLS)

1.1. Versões do TLS

O protocolo tem mais de uma versão, e assim, mais de uma implementação disponível em diversas linguagens de programação. O uso da versão mais recente é recomendável porque ela implementa o estado da arte da segurança em comunicação.

Tabela 1: Versões do TLS

Versão	RFC	Definida em
1.0	2246	1999
1.1	4346	2006
1.2	5246	2008
1.3	8446	2018

1 A especificação OSI está disponível em: https://www.iso.org/ics/35.100/x/

Há uma implementação de TLS em código livre e aberto, o OpenSSL. No lugar de implementar diretamente o TLS, as linguagens de programação podem usar o OpenSSL. A versão estável mais recente do OpenSSL é a série 3.2 com suporte até 23/11/2025. Também está disponível a série 3.1 com suporte até 14/03/2025, e a série 3.0 que é uma versão de suporte de longo prazo (LTS) com suporte até 07/09/2026. Todas as versões mais antigas versões (incluindo 1.1.1, 1.1.0, 1.0.2, 1.0.0 e 0.9.8) agora estão sem suporte e não devem ser usadas. Os usuários dessas versões mais antigas são incentivados a atualizar para 3.2 ou 3.0 o mais rápido possível. O sítio do OpenSSL contém a lista de vulnerabilidades da implementação e quais são as versões que as corrigem. A Tabela 2 mostra em quais versões de OpenSSL foi adicionado suporte às versões de TLS.

Tabela 2: Versões do OpenSSL e suporte a TLS

OpenSSL	Lançamento	Adicionou suporte a TLS
0.9.0	Não houve	1.0
0.9.1	Não houve	1.1
1.0.1	14/03/2012	1.2
3.0	07/09/2021	1.3

SSL é o acrônimo de *Secure Sockets Layer*, um protocolo publicado na versão 2.0 por uma equipe da Netscape liderada pelo criptógrafo egípcio Taher Elgamal, em 1995. O protocolo TLS foi lançado em 1999 como sucessor do SSL 3.0. O TLS é o sucessor direto do SSL, e todas as versões do SSL agora estão obsoletas. No entanto, é comum encontrar o termo *SSL* descrevendo uma conexão TLS. Na maioria dos casos, os termos *SSL* e *SSL/TLS* referem-se ao protocolo TLS e aos certificados TLS. Assim, o OpenSSL deveria se chamar OpenTLS, pois já nasceu após a obsolescência do SSL.

1.2. Versões do Python

A versão estável mais recente do Python é a 3.12.4. É vital que a versão de Python em produção esteja pelo menos na fase de suporte *security*, em que ainda há atualizações para corrigir vulnerabilidades. Recomenda-se, entretanto, a atualização para a versão com com ciclo *bugfix* longo para evitar possíveis explorações de vulnerabilidades pela demora na migração de versões.

O gráfico da Figura 2[2] apresenta o planejamento de suporte das versões de Python até 2030. A próxima versão estável será lançada no final de 2024.

A versão 3.5.3 do Python atualizou o suporte para OpenSSL 1.1.0. Isso quer dizer que, a partir da versão 3.5.3, o Python tinha suporte para TLS 1.0, 1.1 e 1.2. Entretanto, na versão 3.6 do Python, o OpenSSL nas versões 0.9.8, 1.0.0 e 1.0.1 foram tornados obsoletos e não mais suportados. A partir da versão 3.10 do Python, o módulo ssl passou a exigir OpenSSL 1.1.1 ou superior. Isso significa que a partir da versão 3.10, o Python suporta TLS 1.3.

Até a versão 3.6, o Python usava uma única constante para selecionar a mais alta versão do protocolo TLS (ssl.PROTOCOL_TLS) para cliente e servidor. A partir da versão 3.10, foram criadas duas constantes separadas: ssl.PROTOCOL_TLS_CLIENT e ssl.PROTOCOL_TLS_SERVER. O módulo ssl do Python auto-negocia a versão mais alta do protocolo TLS para configurar essas constantes.

A documentação do módulo ssl está disponível em: https://docs.python.org/3/library/ssl.html.

2 https://devguide.python.org/versions/

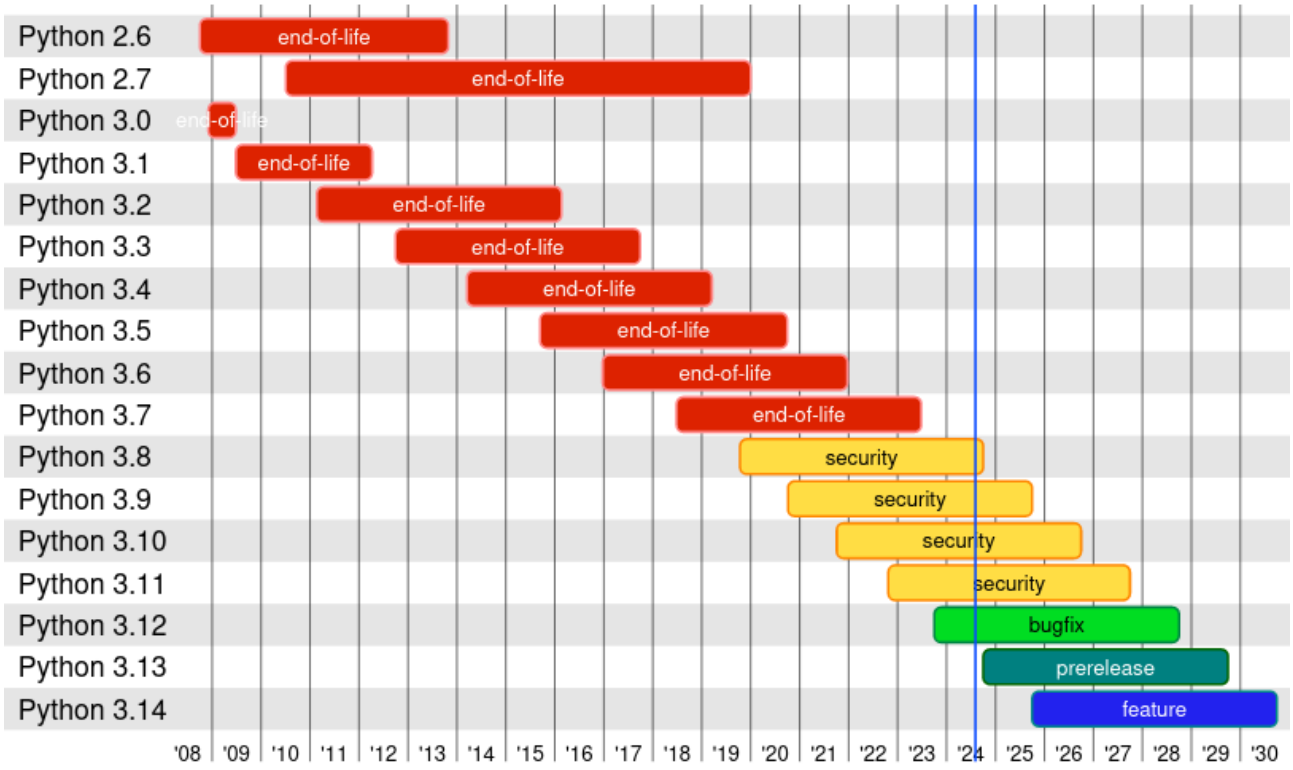

Figura 2: Agenda de suporte para as versões de Python

Para garantir que os aplicativos Python permaneçam seguros, a versão TLS não deve ser codificada permanentemente. Os aplicativos Python devem usar a versão TLS compatível com o sistema operacional (SO).

A recomendação para a construção de aplicações Python é não especificar a versão do TLS, mas configurar o código para permitir que o sistema operacional decida a versão do TLS. É recomendável executar uma auditoria de código completa para verificar se você não está especificando uma versão TLS ou SSL em sua aplicação Python.

2.Análise

Conforme relatamos no capítulo anterior, todas as versões de Python a partir da 3.10 suportam TLS 1.3. A recomendação é que todas as aplicações Python em produção no Serpro utilizem preferencialmente a versão estável com suporte *bugfix* ativo. O uso de versões de Python sem suporte de segurança é um risco para a empresa e para seus clientes.

Considerando que o suporte da versão 3.8 de Python termina no final de 2024, devem ser tomadas providências para migrar as aplicações para a versão 3.12 até o final desse ano. A versão mais antiga com suporte ativo até 2026 é a 3.10.

A existência de versões de Python anteriores à 3.8 é uma situação temerosa, com gravidade inversamente proporcional ao número da versão. Se existem aplicações em produção nessa situação, elas devem ser migradas com máxima urgência. Caso não seja possível uma migração direta para a versão 3.12 por causa do acúmulo de incompatibilidades, a migração pode ser planejada para ser feita mais de uma etapa (por exemplo, migrando para a versão 3.8 e depois para a versão 3.12).

3.Conclusão

Para um uso funcional e seguro de TLS com Python, é recomendável o uso mínimo da versão 3.9, considerando que o suporte ativo será encerrado em alguns meses.
A recomendação para versões de Python inferiores a 3.8 é apenas uma: migração imediata para a versão com suporte ativo mais recente possível.

Este documento foi finalizado em 6 de agosto de 2024.