

OpenSSL



Programm *openssl* für die Kommandozeile

zum Beantragen, Erzeugen und Verwalten von **Zertifikaten**

Aktuelle Version

1.1.1k

25. März 2021

stellt allgemeine kryptographische Funktionen zum Ver- und Entschlüsseln und Tools bereit

nach FIPS 140-2 zertifizierte Open-Source-Programm

Sicherheitsstandard

NIST

ursprünglich *SSL*ey

Message Digest

Cipher commands

umfasst verschiedener Verschlüsselungen

Bemerkenswerte Sicherheitslücken

Schwache Schlüssel unter Debian

13. Mai 2008

Version 0.9.8c-1 bis 0.9.8g-9

Heartbleed-Bug

bis einschließlich 1.0.1f

umfasst Implementierungen der Netzwerkprotokolle

3.0 Release Candidate

17.7.2021

Transport Layer Security

TLS

Vorgängerbezeichnung **Secure Sockets Layer (SSL)**

Verschlüsselungsmodul für Apache-Webserver

mod_ssl

Lizenz

ab Version 3.0.0 steht OpenSSL unter der Apache-2.0-Lizenz

openssl.org/

