Checkvanta

github.com

Sicherheits- und Konfigurationsbericht

Erstellt am: 25.7.2026, 03:56:04 UTC

90
Gesamtscore

Website-Konfiguration

Subscore **90**

TLS

90

- **HTTPS erreichbar** Erforderlich
  Ein HTTPS-Dienst ist erreichbar und hat einen TLS-Handshake abgeschlossen.
- **TLS-Versionen** Erforderlich
  Es werden nur moderne TLS-Versionen (1.2 und/oder 1.3) angeboten.
- **Cipher Suite** Erforderlich
  Die ausgehandelte Cipher Suite (TLS_AES_128_GCM_SHA256) bietet Forward Secrecy.
- **Zertifikat** Erforderlich
  Das Zertifikat ist vertrauenswürdig und für diesen Host gültig.
- **Zertifikatsschlüssel** Erforderlich
  Das Zertifikat verwendet einen starken ECDSA-Schlüssel (256 Bit).
- **Zertifikatssignatur** Erforderlich
  Das Zertifikat verwendet einen sicheren Signaturalgorithmus (ECDSA-SHA256).
- **OCSP-Stapling** Empfohlen · Niedrig
  Der Server liefert keine OCSP-Antwort per Stapling mit.
  Empfehlung: Aktivieren Sie OCSP-Stapling auf dem Webserver.
- **DANE (HTTPS)** Optional · Niedrig
  Für HTTPS sind keine DANE-(TLSA-)Records veröffentlicht.
  Empfehlung: Veröffentlichen Sie bei aktivem DNSSEC TLSA-Records unter `_443._tcp.<host>`, die zu Ihrem Zertifikat passen, und rotieren Sie sie gemeinsam mit dem Zertifikat.
- **Cipher-Reihenfolge** Empfohlen
  Mit TLS 1.3 wählt der Server aus einem kleinen Satz durchweg sicherer Verfahren – die Reihenfolge ist unkritisch.
- **Key Exchange** Erforderlich
  Der Schlüsselaustausch nutzt ECDHE mit Hash SHA256 – Forward Secrecy ist gegeben.
- **TLS-Kompression** Erforderlich
  TLS 1.3 kennt keine Record-Kompression – die Schwachstelle entfällt.
- **Renegotiation** Erforderlich
  TLS 1.3 hat Renegotiation vollständig entfernt – kein Angriffsvektor.
- **Extended Master Secret** Empfohlen
  Der Schlüsselplan von TLS 1.3 ersetzt Extended Master Secret – die Schwäche entfällt.
- **TLS 1.3 0-RTT (Early Data)** Optional
  Der Server akzeptiert kein 0-RTT – die sicherste Voreinstellung.