Checkvanta

cloudflare.com

Sicherheits- und Konfigurationsbericht

Erstellt am: 25.7.2026, 04:25:47 UTC

60
Gesamtscore

Website-Konfiguration

Subscore **60**

TLS

60

- **HTTPS erreichbar** Erforderlich
  Ein HTTPS-Dienst ist erreichbar und hat einen TLS-Handshake abgeschlossen.
- **TLS-Versionen** Erforderlich · Hoch
  Der Server bietet noch eine veraltete TLS-Version (1.0 oder 1.1) an.
  Empfehlung: Deaktivieren Sie TLS 1.0 und 1.1 in Ihrer Webserver- oder CDN-Konfiguration und bieten Sie nur TLS 1.2 und 1.3 an.
- **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 · Niedrig
  Der Server akzeptiert TLS-1.3-0-RTT (max. 14336 Bytes Early Data). Achten Sie auf Replay-Schutz.
  Empfehlung: Aktivieren Sie 0-RTT nur, wenn Ihr Server wirksamen Replay-Schutz bietet und ausschließlich sichere, idempotente Anfragen als Early Data zulässt. Im Zweifel deaktivieren.