Checkvanta

tls-v1-2.badssl.com

Sicherheits- und Konfigurationsbericht

Erstellt am: 25.7.2026, 04:07:50 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_ECDHE_RSA_WITH_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 RSA-Schlüssel (2048 Bit).
- **Zertifikatssignatur** Erforderlich
  Das Zertifikat verwendet einen sicheren Signaturalgorithmus (SHA256-RSA).
- **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
  Der Server erzwingt seine eigene Cipher-Reihenfolge.
- **Key Exchange** Erforderlich
  Der Schlüsselaustausch nutzt ECDHE mit Hash SHA256 – Forward Secrecy ist gegeben.
- **TLS-Kompression** Erforderlich
  TLS-Kompression ist deaktiviert.
- **Renegotiation** Erforderlich
  Der Server unterstützt sichere Renegotiation und lässt keine Client-initiierte Renegotiation zu.
- **Extended Master Secret** Empfohlen · Niedrig
  Der Server unterstützt kein Extended Master Secret.
  Empfehlung: Aktivieren Sie Extended Master Secret in Ihrem TLS-Stack (in aktuellen OpenSSL-/Server-Versionen standardmäßig aktiv) oder wechseln Sie auf TLS 1.3.