Rapport d'analyse SSL/TLS

Cible: drhead.org

Date: *25/03/2025 01:54:20*

Résumé

Problèmes critiques: 0

Avertissements: 1

Configurations correctes: 23

Informations: 12

Avertissements (1)

- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Certificate Transparency: WARNING - Only 2 SCTs included but Google recommends 3 or more

Configurations correctes (23)

- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Certificat valide jusqu'au 2025-06-09
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Algorithme de signature fort: sha256
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Certificat de confiance pour Android CA Store (15.0.0_r9)
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Certificat de confiance pour Java CA Store (jdk-13.0.2)
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Certificat de confiance pour Mozilla CA Store (2024-11-24)
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Certificat de confiance pour Windows CA Store (2023-12-11)
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Bonne pratique: SSL 3.0 désactivé
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Bonne pratique: TLS 1.0 désactivé
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Bonne pratique: TLS 1.1 désactivé
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - TLS 1.2 activé (recommandé)
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Forward Secrecy supporté
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Algorithme RC4 obsolète non supporté
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - TLS 1.3 activé (recommandé)
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Compression TLS désactivée
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Non vulnérable à l'injection OpenSSL CCS
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Supporte TLS Fallback SCSV (protection contre les attaques de rétrogradation)

- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Non vulnérable à Heartbleed
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Non vulnérable à ROBOT
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Non vulnérable aux attaques DoS par renégociation client
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Supporte la renégociation sécurisée
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Reprise de session par ID supportée
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Reprise de session par ticket TLS supportée
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - En-tête HSTS présent

Informations (12)

- Durée du scan: 2.736919 secondes
- Serveur: DRHEAD.ORG:443 (76.76.21.21)
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Nom commun du certificat: drhead.org
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Émetteur du certificat: R11
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - SSL 3.0 non supporté
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - TLS 1.0 non supporté
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - TLS 1.1 non supporté
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - TLS 1.2 supporté avec 4 suites de chiffrement
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - TLS 1.3 supporté avec 3 suites de chiffrement
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Ne supporte pas TLS 1.3 Early Data
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - Durée HSTS: 63072000 secondes
- Serveur: DRHEAD.ORG:443 (76.76.21.21) - HSTS n'inclut pas les sous-domaines

---