TLS Security Assessment

Target: www.cyphers.ai:443
Date: 2/21/2026, 4:22:18 AM
Scan ID: sc_2548e6a2-44c

90

Grade: A

Urgency Breakdown:

5 Low

Certificate Information

Subject: cyphers.ai
Issuer: E7
Valid Until: 4/23/2026
Days Remaining: 61
Key: ECDSA 256-bit

Protocol Support

' TLS 1.0
' TLS 1.1
' TLS 1.2
' TLS 1.3

Security Findings

' Protocol: TLS 1.3 Support
[LOW]
TLS 1.3 is supported

' Certificate: Certificate Validity
[LOW]
Certificate is valid for 61 more days

! Certificate: OCSP Stapling
[LOW]
OCSP stapling is not enabled
Deduction: -5 points
Remediation: Enable OCSP stapling. For nginx: ssl_stapling on; ssl_stapling_verify on;
Why This Matters: Performance optimization that reduces latency for certificate revocation checks. Not a security vulnerability, but improves user experience.

' Headers: HSTS
[LOW]
HSTS is enabled with max-age=31536000 seconds

' Certificate: Certificate Transparency (SCT)
[LOW]
No Signed Certificate Timestamps (SCT) found
Deduction: -5 points
Remediation: Use a CA that supports Certificate Transparency. Most modern CAs include SCTs by default.

Compliance Impact

PCI-DSS 4.2.1: Passing
NDcPP FCS_TLS_EXT.1: Passing
HIPAA: Passing