TLS Security Assessment

Target: emp.cellcrypt.io:443
Date: 2/18/2026, 7:42:31 PM
Scan ID: sc_5b058744-0c7

80

Grade: B

Urgency Breakdown:

1 Medium | 4 Low

Certificate Information

Subject: api.cellcrypt.io
Issuer: R12
Valid Until: 4/27/2026
Days Remaining: 67
Key: RSA 2048-bit

Protocol Support

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

Security Findings

' Headers: HSTS
[MEDIUM]
HTTP Strict Transport Security (HSTS) header is not set
Deduction: -10 points
Remediation: Add HSTS header. For nginx: add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload";
Why This Matters: First-time visitors can be intercepted via man-in-the-middle attacks. Critical for authentication endpoints where credentials are transmitted.

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

' Certificate: Certificate Validity
[LOW]
Certificate is valid for 67 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.

' 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: 1 failure(s)
NDcPP FCS_TLS_EXT.1: Passing
HIPAA: Passing