TLS Security Assessment

Target: vestd.com:443
Date: 2/18/2026, 7:50:23 PM
Scan ID: sc_7afbf036-fa3

5

Grade: F

Urgency Breakdown:

2 Critical | 2 High | 5 Low

Certificate Information

Subject: vestd.com
Issuer: WE1
Valid Until: 4/20/2026
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 1.0 Enabled
[CRITICAL]
TLS 1.0 is enabled - deprecated and insecure
Deduction: -25 points
Remediation: Disable TLS 1.0 in server configuration. For nginx: ssl_protocols TLSv1.2 TLSv1.3;
Why This Matters: Enables downgrade attacks. Large providers keep TLS 1.0 for legacy compatibility with extensive monitoring. Typical servers lack this oversight and are fully exploitable.

' Vulnerability: BEAST (CVE-2011-3389)
[CRITICAL]
Server vulnerable to BEAST attack
Deduction: -25 points
Remediation: Disable TLS 1.0 or remove CBC ciphers. Prefer TLS 1.2+ with GCM or ChaCha20.
Why This Matters: Large enterprises like Google mitigate BEAST with hardened implementations and client-side fixes. Most servers don't have these safeguards - if this were your server, traffic could be decrypted.

' Protocol: TLS 1.1 Enabled
[HIGH]
TLS 1.1 is enabled - deprecated and insecure
Deduction: -25 points
Remediation: Disable TLS 1.1 in server configuration. For nginx: ssl_protocols TLSv1.2 TLSv1.3;
Why This Matters: Deprecated protocol with known weaknesses. Should be disabled on all production servers to prevent protocol downgrade attacks.

' Vulnerability: SWEET32 (CVE-2016-2183)

[HIGH]
Server vulnerable to SWEET32 birthday attack on 64-bit block ciphers
Deduction: -15 points
Remediation: Remove 3DES cipher suites. Use AES-GCM or ChaCha20-Poly1305 instead.

' 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 enabled

' 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: 3 failure(s)
NDcPP FCS_TLS_EXT.1: 2 failure(s)
HIPAA: Passing