harbourline.example

SSL/TLS Check | 13 October 2026, 06:40 UTC

B

Overall grading 80/100

The certificate is valid and the protocols are current, but it expires in 16 days.

Grade driven by: Certificate expires in 16 days

1
MEDIUM

About this check

What we checked

We connected to this server the way a browser does and examined the certificate it presented and the encryption it agreed to use: who issued the certificate, whether it is still valid and matches the name, which protocol versions the server still accepts, and which encryption ciphers it will agree to. We also probed for a set of named weaknesses by name.

Why it matters

A certificate that has expired or does not match the name makes browsers warn your visitors, and most of them will leave. Obsolete protocols and broken ciphers are worse and quieter: the padlock still appears, while somebody positioned between your visitor and your server can read or alter what passes.

How to read the grade

The grade follows the most serious problem found, not an average. Genuinely broken encryption is an F here — a padlock that means nothing is not a C. A clean setup that also tells browsers to refuse plain HTTP for at least six months earns A+.

Findings (1)

MEDIUM

Expiring Certificate — Your certificate expires in 16 days

CWE-298

It's still valid, but expiry is approaching.

Confirmed - tested directly; the server behaved this way.

What to do

Schedule a renewal or confirm auto-renewal is enabled.

Full scan detail

The complete technical data behind the findings above — the same detail the app shows in its expandable panels. Use your PDF viewer's outline to jump between sections.

Resolved addresses

Address tested	`203.0.113.40`

Certificate details

The certificate the server presented, and how it validated.

Issued for	harbourline.example
Issued by	Example Trust CA R4
Valid from	1 August 2026
Valid until	30 October 2026
Days until expiry	16
Expired	No
Hostname match	Matches the certificate
Self-signed	No
Chain trusted	Trusted to a known root
Public key	ECDSA 256-bit
Signature algorithm	ECDSA-SHA256
Negotiated protocol	TLS 1.3
Negotiated cipher	TLS_AES_128_GCM_SHA256
Protocol support	SSL 3.0 off, TLS 1.0 off, TLS 1.1 off, TLS 1.2 on, TLS 1.3 on
OCSP stapling	Stapled in the handshake
ALPN (application protocol)	h2

Subject alternative names

`harbourline.example, www.harbourline.example, portal.harbourline.example`

Named-weakness checks

Each known weakness we probe for. "Not tested" means we could not get a definite answer on the wire — it is not a pass.

OK **Heartbleed (CVE-2014-0160)**

The server did not return memory to a malformed heartbeat.

OK **CCS injection (CVE-2014-0224)**

An early ChangeCipherSpec was refused.

OK **ROBOT (Bleichenbacher oracle)**

No RSA key exchange is offered.

OK **POODLE (SSLv3)**

SSL 3.0 is refused.

OK **DROWN (SSLv2)**

SSLv2 is refused.

OK **Secure renegotiation (RFC 5746)**

Supported.

OK **CRIME (TLS compression)**

Compression is off.

OK **Weak Diffie-Hellman / Logjam**

No finite-field Diffie-Hellman suite is offered.

Accepted cipher suites

Suites the server accepted from us, one row per protocol version — weakest first. The DHE, ARIA, Camellia and SEED families are offered as well as the common ones, so a family missing here is one the server did not accept. It is still not every suite that exists, so a very unusual one may not appear. TLS 1.3 is the one exception to listing only what was demonstrated — its three suites cannot be offered individually, so all three are listed whenever TLS 1.3 handshakes.

6 strong

Version	Cipher suite	Strength	Fwd secrecy
TLS 1.2	`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`	STRONG	Yes
TLS 1.2	`TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`	STRONG	Yes
TLS 1.2	`TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256`	STRONG	Yes
TLS 1.3	`TLS_AES_128_GCM_SHA256`	STRONG	Yes
TLS 1.3	`TLS_AES_256_GCM_SHA384`	STRONG	Yes
TLS 1.3	`TLS_CHACHA20_POLY1305_SHA256`	STRONG	Yes

Report generated 17 October 2026, 19:36 UTC. Scan reference f2fda325-396a-4a83-8742-78bce44abeac.