SSL/TLS Configuration Report

Target: juice-shop.herokuapp.com:443 | **Generated:** 2025-09-08_19-06-00

Findings: 1 (High risk: 0)

Vulnerabilities / Findings

Issue	Status	Risk	Evidence	Mitigation
Broad Wildcard Certificate	Info	Low	Wildcard used with minimal SAN entries	Limit wildcard certificates; prefer SAN certificates scoped to required hosts only.

Protocol Support

Protocol	Supported
TLSv1.0	❌
TLSv1.1	❌
TLSv1.2	✅
TLSv1.3	✅

Certificate Info

Subject	*.herokuapp.com
Issuer	Amazon RSA 2048 M02
Valid From	Jan 31 00:00:00 2025 GMT
Valid To	Mar 1 23:59:59 2026 GMT
Days Until Expiry	174
Wildcard	Yes
Self-Signed	No
Host Match	Yes