Minimum iOS Version Required to Avoid SSL Certificate Errors on iPhones

Issue Summary

A user accessing your WordPress site with an iPhone running iOS 8 and using the Safari browser is receiving an error about an invalid security certificate. The same pages do not show errors on up-to-date desktop browsers, indicating the certificate is valid but not recognized by older devices.

Root Cause

- iOS 8 is outdated and does not include modern root certificates like ISRG Root X1 (used by Let's Encrypt).
- It may also lack support for TLS 1.2 or 1.3, which are now required by many secure websites.
- As a result, even valid certificates may be flagged as invalid on old systems.

Minimum iOS Version Recommendation

To ensure compatibility with modern SSL certificates and avoid security warnings:

- - Minimum iOS version: iOS 12.2
  - Includes updated root certificates and TLS 1.2 support.
  - Recommended iOS version: iOS 14 or later
  - Ensures long-term compatibility and full support for TLS 1.3 and modern cryptographic standards.

Suggestions for the User

- Update the iPhone to at least iOS 12.2 (if supported).
- If an update is not possible:
  - Try using a different browser like Firefox for iOS.
  - Access the site from a newer device.

Optional Technical Workaround (Not Recommended)

Some certificate authorities (like Let’s Encrypt) used to support cross-signing with older roots like DST Root CA X3, but these have expired or been deprecated. Modifying your certificate chain to include legacy support is possible, but discouraged due to security risks and lack of future support.

Contact your hosting provider or certificate authority if you need help verifying your certificate chain.