PAUBOX RESEARCH

PAUBOX

Amazon SES blocked 0 of 4 invalid certificates

SES completed encrypted sessions to self-signed, expired, and mismatched certificates without aborting the connection.

What we found

A completed TLS handshake proves encryption, not that the recipient is who they claim to be.

TLS does two jobs: it encrypts the message and it verifies the receiving server through its certificate. Amazon SES does the first and skips the second. It accepted self-signed, expired, and hostname-mismatched certificates under both configurations, leaving an encrypted session open to an unverified recipient.

What it means for buyers

Self-signed certificates pass
SES delivers to a certificate the receiver signed itself, with no trusted authority involved.

Expired certificates pass
An expired certificate does not stop delivery under either SES configuration.

The door opens to interception
An attacker presenting a fake certificate can receive PHI while the sender sees success.

WHY PAUBOX

#1

on G2 for email encryption in healthcare, rated by verified users.

Recipient certificates are validated
Paubox confirms a valid certificate before delivery, so PHI reaches the verified recipient.

A verified, encrypted connection
PHI transits only over a session that is both encrypted and authenticated.

HITRUST certified
Annual third-party audit of every control.

Sources: Paubox 2026 research, How Amazon SES puts PHI at risk | Amazon SES Developer Guide (April 2026).