**Threat:** Replay Attacks  
**Affected Component:** Communication Protocol - All Requests and Responses  
**Module Details:** TCP communication layer  
**Vulnerability Class:** Replay Attack Vulnerability  
**Description:** Lack of measures to prevent the replay of messages. Without timestamps or sequence numbers, messages can be replayed by an attacker to the server, which might process them as legitimate.  
**Result:** Unauthorized actions might be executed if an attacker replays previous requests, such as file transfers or public key exchanges.  
**Prerequisites:** Attacker must be able to intercept and resend valid protocol messages.  
**Business Impact:** Data integrity issues, unauthorized actions being processed, and resource wastage due to repeated message processing.  
**Proposed Remediation:** Introduce nonce or timestamp and sequence numbers in the protocol. Implement server-side checks to discard duplicate or out-of-order messages.

**Threat:** Man-in-the-Middle (MitM) during Key Exchange  
**Affected Component:** Key Exchange Mechanism  
**Module Details:** Public Key Transmission (Request code 1026)  
**Vulnerability Class:** Man-in-the-Middle Vulnerability  
**Description:** Public keys are transmitted without integrity checks or endpoint authentication, making them susceptible to interception and replacement.  
**Result:** An attacker could replace legitimate keys with their own, decrypting and altering messages without detection.  
**Prerequisites:** Attacker has access to the communication channel during key exchange.  
**Business Impact:** Compromise of confidentiality and integrity, leading to potential data breaches and system compromise.  
**Proposed Remediation:** Use certificate-based authentication for public keys. Implement Transport Layer Security (TLS) to protect the key exchange process.

**Threat:** Inadequate RSA Key Size  
**Affected Component:** Asymmetric Encryption Implementation  
**Module Details:** RSA Key Generation  
**Vulnerability Class:** Weak Cryptographic Standards  
**Description:** The protocol allows for RSA keys of sizes that may not be secure against modern cryptographic attacks.  
**Result:** Encrypted communications could be broken, exposing sensitive data.  
**Prerequisites:** Attacker with sufficient computational power.  
**Business Impact:** Potential for significant data breaches, undermining user trust and leading to regulatory scrutiny.  
**Proposed Remediation:** Mandate a minimum RSA key size of 2048 bits in line with current best practices.

**Threat:** IV Reuse in AES-CBC Encryption  
**Affected Component:** Symmetric Encryption Scheme  
**Module Details:** AES-CBC Encryption Process  
**Vulnerability Class:** Insufficient Cryptographic Protection  
**Description:** The protocol specifies that the initialization vector (IV) for AES-CBC is always reset, which may lead to IV reuse.  
**Result:** Reusing an IV with the same key can compromise the security of the encryption, potentially revealing patterns in the plaintext.  
**Prerequisites:** Attacker has access to multiple ciphertexts encrypted with the same key-IV pair.  
**Business Impact:** Possible decryption of sensitive data leading to information disclosure and privacy breaches.  
**Proposed Remediation:** Implement random, unique IVs for each encryption operation. Avoid IV reuse across sessions and messages.