- **Threat**
  Spoofing the Server to Extract Sensitive Client Information

- **Affected Component**
  Authentication, Files
- **Vulnerability Class**
  CWE-300 - Channel Accessible by Non-Endpoint
- **Description**
  Attackers can disguise themselves as a legitimate host and intercept the communication between the client and server. By acting as a middleman, the attacker can manipulate the information exchange. If the client mistakenly trusts the attacker, it might use their encryption keys (AES for e.g.), inadvertently sending confidential files.
- **Result**
  The client may connect to a malicious server without realizing it and transmit sensitive data like UUIDs or secret files.
- **Prerequisites**
  The attacker needs access to the client's network to perform ARP spoofing or other interception techniques.
- **Business Impact**
  Personal information could leak to unintended third parties, leading to reputational or financial damage.
- **Proposed Remediation**
  Implement server-side certificates and ensure that clients validate them correctly.
- **Risk Evaluation**
  - AV: Network
  - AC: Low
  - PR: None
  - UI: Required
  - Scope: Unchanged
  - Confidentiality (C): High
  - Integrity (I): High
  - Availability (A): None
  - Overall Risk: 8.0 [High]

- **Threat**
  Lack of Encryption for Stored Files
- **Affected Component**
  File Storage
- **Vulnerability Class**
  CWE-311 - Missing Encryption of Sensitive Data
- **Description**
  Files uploaded by clients are stored on the server in plaintext, meaning they are not encrypted at rest. If an attacker gains unauthorized access to the storage directory or the server filesystem, they could view, copy, or tamper with sensitive files without any restrictions. This issue is exacerbated by the use of a simple folder structure without access controls or encryption mechanisms.
- **Result**
  An attacker with access to the storage can read confidential information, alter files, or inject malicious content, potentially leading to data breaches or compromised system integrity.
- **Prerequisites**
  The attacker needs access to the server's storage, either through exploitation or physical access.
- **Business Impact**
  Exposure of sensitive information, data tampering, and reputational damage. It could also result in compliance violations if personal or regulated data is compromised.
- **Proposed Remediation**
  Encrypt files stored on the server using AES or another strong encryption algorithm. Implement access control to restrict unauthorized access to storage directories and periodically monitor and audit file storage for suspicious access or modifications.
- **Risk Evaluation**
  - AV: Local
  - AC: Low
  - PR: Low
  - UI: None
  - Scope: Unchanged
  - Confidentiality (C): High
  - Integrity (I): High
  - Availability (A): Medium
  - Overall Risk: 7.3 [High]

- **Threat**
  Private Key Exposure

- **Affected Component**
  Files
- **Vulnerability Class**
  CWE-1125 - Excessive Attack Surface
- **Description**
  The private key is stored in multiple files, increasing the attack surface and making synchronization more difficult. If an attacker gains access to these files, they can extract the AES key and perform unauthorized actions on behalf of the legitimate user.
- **Result**
  Unauthorized access to the private key files could enable attackers to compromise the client's identity and data.
- **Prerequisites**
  The attacker needs access to the unprotected key files on the client's machine.
- **Business Impact**
  Sensitive information could be exposed, leading to potential misuse of the client's identity and data.
- **Proposed Remediation**
  Secure the private keys by encrypting and limiting their storage locations.
- **Risk Evaluation**
  - AV: Network
  - AC: Low
  - PR: None
  - UI: None
  - Scope: Unchanged
  - Confidentiality (C): None
  - Integrity (I): None
  - Availability (A): High
  - Overall Risk: 7.5 [High]

- **Threat**
  Lack of Proper Error Handling Leading to Information Disclosure
- **Affected Component**
  Server Communication
- **Vulnerability Class**
  CWE-209 - Information Exposure Through an Error Message
- **Description**
  The server prints detailed error messages, such as "server responded with an error", during communication failures. This includes the possibility of the client repeatedly attempting a failed operation (up to 3 times) before termination. If these error messages contain sensitive details or internal system information, attackers could gather insights about the server's configuration or vulnerabilities.
- **Result**
  Attackers can exploit the error messages to learn about the server's structure or discover specific weaknesses, such as misconfigurations, active services, or exposed file paths.
- **Prerequisites**
  The attacker must trigger specific server conditions that generate detailed error responses.
- **Business Impact**
  The leakage of system information could lead to targeted attacks, increased exposure to exploits, and compromised service availability.
- **Proposed Remediation**
  Replace detailed error messages with generic responses like "An error occurred. Please try again.", log detailed information for developers internally, without exposing it to the client and implement rate limiting on retries to prevent exploitation through repeated failed requests.
- **Risk Evaluation**
  - AV: Network
  - AC: Low
  - PR: None
  - UI: Required
  - Scope: Unchanged
  - Confidentiality (C): Low
  - Integrity (I): Low
  - Availability (A): Low
  - Overall Risk: 5.8 [Medium]

- **Threat**
  Weak Authentication via Easily Guessable Credentials

- **Affected Component**
  Authentication
- **Vulnerability Class**
  CWE-1391 - Use of Weak Credentials
- **Description**
  Authentication relies on UUID and a client name, but these are insufficiently secure. The UUID, though long, might not be generated with strong cryptographic randomness, making it vulnerable to guessing attacks. The client's name, on the other hand, is unprotected and easily obtainable. Additionally, these credentials are saved in unprotected files on the client's machine, further increasing the risk of unauthorized access.
- **Result**
  An attacker can obtain the credentials by intercepting the network traffic or accessing files on the client's machine.
- **Prerequisites**
  The attacker needs access to either the network or the client's stored credential files.
- **Business Impact**
  Data loss, unauthorized access, and the possibility of the client being locked out of their account.
- **Proposed Remediation**
  Adopt stronger authentication methods, such as OTP, instead of relying on UUID alone.
- **Risk Evaluation**
  - AV: Network
  - AC: Low
  - PR: None
  - UI: Required
  - Scope: Unchanged
  - Confidentiality (C): High
  - Integrity (I): High
  - Availability (A): High
  - Overall Risk: 8.8 [High]

- **Threat**
  Server Downtime from DoS or DDoS Attacks

- **Affected Component**
  All Server Functions
- **Vulnerability Class**
  CWE-400 - Uncontrolled Resource Consumption
- **Description**
  Since the protocol lacks mechanisms for rate limiting or congestion control, it becomes susceptible to attacks that flood the server with a massive volume of requests.
- **Result**
  A DoS or DDoS attack can overwhelm the server, making it unresponsive to legitimate users.
- **Prerequisites**
  The attacker needs the capability to send a large number of requests to the server.
- **Business Impact**
  Service availability is affected, preventing legitimate users from accessing the server.
- **Proposed Remediation:**
  Restricting the number of concurrent connections to protect resource and setting the rate limits on requests (some kind of a delay) to prevent excessive usage.
- **Risk Evaluation**
  - AV: Network
  - AC: Low
  - PR: None
  - UI: None
  - Scope: Unchanged
  - Confidentiality (C): None
  - Integrity (I): None
  - Availability (A): High
  - Overall Risk: 7.5 [High]

- **Threat**
  Credentials Exposed in Plain Text

- **Affected Component**
  Authentication
- **Vulnerability Class**
  CWE-319 - Cleartext Transmission of Sensitive Data
- **Description**
  The UUID and the client's name, which are needed to log in, are transmitted without encryption, exposing them to theft. An attacker could easily intercept this data during transit.
- **Result**
  If an attacker intercepts the credentials, they could impersonate the client, perform actions like exchanging keys or sending files, and potentially overwrite or expose files during transmission.
- **Prerequisites**
  Attackers can monitor and intercept network traffic to obtain credentials.
- **Business Impact**
  The theft of credentials could lead to data loss, service disruption, and unauthorized access.
- **Proposed Remediation**
  Use secure protocols like TLS to encrypt all transmitted data.
- **Risk Evaluation**
  - AV: Network
  - AC: Low
  - PR: None
  - UI: Required
  - Scope: Unchanged
  - Confidentiality (C): High
  - Integrity (I): High
  - Availability (A): High
  - Overall Risk: 8.7 [High]