# Hadas tapiro 325960912

# Detailed Security Vulnerability Report

This report provides a detailed analysis of potential vulnerabilities within the communication protocol, along with possible threats, impacts, and recommended mitigation strategies.

## Key Transmission Without Authentication

|  |  |
| --- | --- |
| Name | Key Transmission Without Authentication |
| Description | The client sends a public key to the server without additional verification. |
| Impact | MITM (Man-In-The-Middle) attacks may occur where an attacker intercepts and replaces the public key, allowing decryption of communications. |
| Proposed Remediation | Add digital certificates or two-factor authentication to ensure the client’s identity. |
| Risk | High |
| Exploitability | Medium |
| Discoverability | High |
| Affected Users | All clients using the protocol |
| Business Impact | Loss of data integrity and confidentiality. |

## Reliance on CRC for File Verification

|  |  |
| --- | --- |
| Name | Reliance on CRC for File Verification |
| Description | CRC-based file verification may not be robust enough to ensure file integrity. |
| Impact | An attacker could alter the file contents and craft a matching CRC, effectively spoofing the file. |
| Proposed Remediation | Use a digital signature based on a private key to authenticate the transmitted content. |
| Risk | High |
| Exploitability | Medium |
| Discoverability | Medium |
| Affected Users | All clients transmitting files |
| Business Impact | Potential for corrupted or tampered file transmission. |

## AES Keys Stored in Plain Memory

|  |  |
| --- | --- |
| Name | AES Keys Stored in Plain Memory |
| Description | AES encryption keys are stored in memory without additional encryption. |
| Impact | A server compromise could lead to direct access to keys, allowing decryption of sensitive data. |
| Proposed Remediation | Encrypt the keys in memory and clear memory upon process termination. |
| Risk | Critical |
| Exploitability | High |
| Discoverability | Medium |
| Affected Users | All clients and data in transit |
| Business Impact | Major data breach and compromise of secure information. |

## Sensitive Information Stored in Plaintext Files

|  |  |
| --- | --- |
| Name | Sensitive Information Stored in Plaintext Files |
| Description | Keys and passwords are stored in plaintext files on the system. |
| Impact | An attacker gaining access to these files can easily access sensitive data. |
| Proposed Remediation | Encrypt sensitive files and store in a secure database (e.g., HSM). |
| Risk | High |
| Exploitability | Medium |
| Discoverability | High |
| Affected Users | All users |
| Business Impact | Potential data leakage and unauthorized access to confidential information. |

## Requests Lacking Unique Identification

|  |  |
| --- | --- |
| Name | Requests Lacking Unique Identification |
| Description | Requests lack unique identifiers like signatures or nonce values. |
| Impact | Replay attacks are possible, where previously sent client messages can be reused by an attacker. |
| Proposed Remediation | Add timestamps and nonce values to ensure request uniqueness and mitigate replay attacks. |
| Risk | Medium |
| Exploitability | Medium |
| Discoverability | Medium |
| Affected Users | All users |
| Business Impact | Increased vulnerability to unauthorized actions or message replay. |

## No Limit on Connection Attempts

|  |  |
| --- | --- |
| Name | No Limit on Connection Attempts |
| Description | The protocol lacks a limit on the number of allowed connection attempts. |
| Impact | Brute-force attacks could allow unauthorized access to the system. |
| Proposed Remediation | Implement a login attempt limit with account lockout after consecutive failed attempts. |
| Risk | Medium |
| Exploitability | High |
| Discoverability | Medium |
| Affected Users | All users |
| Business Impact | Potential unauthorized access and brute-force risk. |

## Fixed IV in AES-CBC Encryption

|  |  |
| --- | --- |
| Name | Fixed IV in AES-CBC Encryption |
| Description | Using a fixed IV in AES-CBC encryption weakens encryption security. |
| Impact | Pattern-based attacks may decipher parts of the encrypted content. |
| Proposed Remediation | Use a random IV for each encryption or add an additional encryption layer. |
| Risk | High |
| Exploitability | High |
| Discoverability | Medium |
| Affected Users | All users |
| Business Impact | Compromised confidentiality of sensitive data. |