1)Lack of Rate Limiting or Reconnection Delays

- Threat: Brute force attacks

.

- Affected Component: Server's client reconnection handling.

- Module Details: Reconnection (Code 1027).

- Vulnerability Class: DoS and brute force attacks.

- Description: Without rate limiting or delay, an attacker can repeatedly attempt to reconnect, overwhelming the server.

- Result: Denial of Service or potential unauthorized access.

- Prerequisites: Basic scripting and network connection.

- Business Impact: Server downtime, potential data breach.

- Proposed Remediation: Implement rate limiting and exponential backoff for reconnect attempts.

- Risk:

Damage Potential: 8 (Repeated reconnections can lead to server overload)
Reproducibility: 10 (Easily repeatable with simple scripts)
Exploitability: 8 (No advanced knowledge required, just persistence)
Affected Users: 10 (All users affected if the server goes down)
Discoverability: 9 (Easily testable and observable)
Overall: 9.0

אין הגבלה על מספר הבקשות או מנגנון CAPTCHA

חולשה: הפרוטוקול אינו מכיל הגנות מובנות נגד התקפות ברוט-פורס או התקפות אוטומטיות.
התקפה אפשרית: מתקיף יכול להציף את השרת בבקשות, מה שעלול להוביל להשבתת השירות.
הצעה לתיקון: יש להטמיע מנגנונים להגבלת מספר הבקשות ואתגרי CAPTCHA במקרים של פעילות חשודה או בתדירות גבוהה.

2. No Encryption for Name during Subscription

- Threat: Eavesdropping on network to grab usernames.

- Affected Component: Initial subscription.

• Module Details: Subscription (Code 1025).

• Vulnerability Class: Data interception.

• Description: Usernames might be intercepted during transmission.

• Result: Unauthorized name access.

• Prerequisites: Ability to sniff network traffic.

• Business Impact: Exposure of user details.

• Proposed Remediation: Encrypt the entire communication, not just sensitive data.

• Risk:

Damage Potential: 7 (Names can be sensitive)
Reproducibility: 8 (Easily repeatable in the correct network position)
Exploitability: 6 (Requires network access and sniffing tools)
Affected Users: 7 (Users attempting to subscribe)
Discoverability: 7 (Requires some network monitoring tools)
Overall: 7.0

חיבור מחודש באמצעות שם בלבד:
חולשה: החיבור המחודש דורש רק את שם הלקוח, אשר אינו מבטיח ייחודיות או אבטחה.
התקפה אפשרית: התקפות התחזות בהן המתקיף מתחבר מחדש באמצעות שם של משתמש אחר.
הצעה לתיקון: השתמש במזהה הלקוח הייחודי או הצג אימות דו-גורמי עבור החיבור המחודש.

3. Undefined Size for Encrypted AES Key

• Threat: Buffer overflows or underflows.

• Affected Component: Key handling.

• Module Details: Receiving encrypted AES key (Code 2102).

• Vulnerability Class: Buffer overflow.

• Description: Undefined sizes can lead to memory issues on the server/client.

• Result: Potential remote code execution or data corruption.

• Prerequisites: Knowledge of memory vulnerabilities and exploitation.

• Business Impact: Server compromise or data loss.

• Proposed Remediation: Clearly define and validate key sizes.

• Risk:

Damage Potential: 9 (Buffer overflows can lead to full server compromise)
Reproducibility: 7 (Might require knowledge of specific server setup)
Exploitability: 7 (Requires advanced knowledge)
Affected Users: 9 (All users trusting the server)
Discoverability: 6 (Requires specific tests and potential reverse engineering)
Overall: 7.6

אורך מפתח AES לא מוגדר ושיטת הצפנה להחלפת המפתח:

חולשה: ללא הגדרת אורך מפתח AES, יש סיכון לשימוש בהצפנה פחות חזקה.
התקפה אפשרית: התקפות ברוט-פורס הופכות ליותר אפשריות כאשר מדובר באורך מפתח AES קצר יותר.
הצעה לתיקון: ציין ואכוף את השימוש ב-AES-256 להצפנה סימטרית ואמץ פרוטוקולים בטוחים להחלפת מפתח כמו Diffie-Hellman.

4**. No Explicit Validation on File Name Length**

• Threat: Buffer overflows.

• Affected Component: File handling.

• Module Details: Sending a file (Code 1028).

• Vulnerability Class: Buffer overflow.

• Description: Without explicit checks, overly long file names can overflow buffers.

• Result: Potential data corruption or remote code execution.

• Prerequisites: Basic file manipulation.

• Business Impact: Data corruption or server compromise.

• Proposed Remediation: Validate file name lengths and truncate or reject overly long names.

• Risk:

Damage Potential: 9 (Potential server compromise)
Reproducibility: 8 (Easily reproducible if the length isn't checked)
Exploitability: 7 (Requires crafting a malicious file name)
Affected Users: 8 (Users attempting to send/receive files)
Discoverability: 7 (Testable with large file names)
Overall: 7.8

אין ולידציה ברורה לאורך שם הקובץ
חולשה:

המערכת איננה בודקת את אורך שם הקובץ. זה יכול להוביל לפגיעות של התקפת גלישת חוצץ (buffer overflow).
התקפה אפשרית:

התקפת גלישת חוצץ בעקבות שליחת קובץ עם שם ארוך מדי. ההתקפה עלולה לגרום לפגיעה בנתונים או להרצת קוד זר.

הצעה לתיקון:

הוספת בדיקה לאורך שם הקובץ ודחייה או קיצוץ של שמות קבצים ארוכים מדי.

5. CRC as Sole File Integrity Mechanism

• Threat: Undetected file tampering.

• Affected Component: File handling.

• Module Details: Sending and receiving files (Codes 1028, 1029, 1030).

• Vulnerability Class: Integrity breach.

• Description: CRCs can be fooled to allow tampered files to appear legitimate.

• Result: Reception of tampered files.

• Prerequisites: Knowledge of CRC weaknesses.

• Business Impact: Data tampering without detection.

• Proposed Remediation: Implement stronger cryptographic hashes for file integrity.

• Risk:

Damage Potential: 8 (Tampered files can be harmful)
Reproducibility: 7 (Requires specific knowledge of CRC and file tampering)
Exploitability: 6 (Requires some cryptographic knowledge)
Affected Users: 8 (Users sending/receiving files)
Discoverability: 6 (Requires testing with tampered files)
Overall: 7.0

אין אוטנטיקציה מפורשת לשלמות הקובץ:

חולשה: הסתמכות באופן בלעדי על CRC לשלמות הקובץ.
התקפה אפשרית: מתקיף עשוי לשנות את הקובץ ולהתאים את ה-CRC כך שהוא יעבור את בדיקת השלמות.

הצעה לתיקון: לצד ה-CRC, יש להטמיע גיבוב קריפטוגרפי וחתימות דיגיטליות להעברות הקבצים.

6. Undefined Encryption Algorithms

• Threat: Usage of weak or deprecated encryption.

• Affected Component: Key exchanges and file/message transmissions.

• Module Details: Sending a file (Code 1028) and encrypted key exchanges (Code 2102).

• Vulnerability Class: Ambiguous encryption standards.

• Description: The protocol doesn't specify which encryption algorithms are used, leading to the potential use of weak or broken encryption methods.

• Result: Compromised data integrity and confidentiality.

• Prerequisites: Knowledge of encryption and potential weaknesses.

• Business Impact: Exposed data, loss of trust.

• Proposed Remediation: Clearly specify and mandate modern, industry-accepted encryption algorithms.

• Risk:

Damage Potential: 9 (Weak or deprecated encryption can lead to significant data breaches)
Reproducibility: 8 (If encryption is weak or broken, it can be repeatedly exploited)
Exploitability: 7 (Requires some knowledge of encryption, but many tools exist for breaking weak encryption)
Affected Users: 9 (All users trusting the encryption can be affected)
Discoverability: 7 (Requires some knowledge and monitoring, but generally discoverable)
Overall: 8.0

הצפנה סימטרית להעברת הודעות:

חולשה: השימוש בהצפנה סימטרית הופך את ההודעות לפגיעות להתקפות MITM אם המפתח נפגע.
התקפה אפשרית: התקפות "איש באמצע" בהן המתקיף "חוטף " ואולי משנה הודעות בין לקוחות.
הצעה לתיקון: אמץ שיטות הצפנה מקצה לקצה והחלף באופן תדיר את המפתחות הסימטריים.

7. **Replay Attack Vulnerability**

• Threat: Re-sending a valid data transmission to trick the system.

• Affected Component: All communication, particularly key exchanges and subscriptions.

• Module Details: Subscription (Code 1025), Sending a public key (Code 1026), Reconnecting (Code 1027).

• Vulnerability Class: Unauthorized data replay.

• Description: Without a mechanism to detect repeated data, attackers can replay old transmissions to perform unauthorized operations.

• Result: Unauthorized actions, potential data breaches.

• Prerequisites: A previously captured valid request or transmission.

• Business Impact: Unauthorized operations, potential data alterations.

• Proposed Remediation: Introduce time stamps, sequence numbers, or one-time tokens in the protocol.

• Risk:
  Damage Potential: 8
  Reproducibility: 7
  Exploitability: 7
  Affected Users: 8
  Discoverability: 7
  Overall: 7.4

חולשה: אין מנגנון לזיהוי שידורי נתונים חוזרים, מה שהופך את המערכת לפגיעה להתקפות Replay.
התקפה אפשרית: שידור מחדש של הודעה תקינה בכדי לרמות את המערכת.
הצעה לתיקון: הוספת חותמות זמן, מספרי סידור או אסימון לשימוש חד פעמי בפרוטוקול.