Threat	Denial of service
Affected component	login mechanism in the server
Module details	Reconnect module
Vulnerability class	?
Description	The protocol states that reconnect request is based on user name alone, so the attacker can pretend to be any user he knows, and change their symmetrical key to deny them from completing the current session and force them to reconnect again.
Result	Attacker disrupt users from completing sessions
Prerequisites	Attacker has can communicate with the server, and knows the names of the users he want to deny service from.
Business impact	Users cant use the server
Proposed remediation	Use private key to sign request to reconnect to prove autenticity
Risk	Damage potential: 8 Reproducibility: 10 Exploitability: 7 Affected users: 9 Discoverability: 10

Threat	Denial of service, exhaustion of resources
Affected component	File decrypting & checksum & saving mechanisms
Module details	File decrypting & checksum & saving mechanisms
Vulnerability class	?
Description	The protocol states a very large (implict) limit to file size, which is around 300TB (32 bits describes packet size and 16 bits to describe packet count) sending such a big file to the server will probably block its processing capacity for a very long time and fill up the storage quickly. To save resources the attacker can stream random bits to the request to skip storing the whole “file” in memory & encrypting it. Checksum can be calculated on the fly as well to make sure the server will actually try to save the file to disk, but then the attacker needs to encrypt as well, which will require more resources .
Result	Server resources run out completely, preventing any other user from getting service and potentially taking the server down.
Prerequisites	Attacker has can communicate with the server, and have sufficient bandwidth to send all the data.
Business impact	Users cant use the server
Proposed remediation	Ratelimit file transfer, lower max size of the files.
Risk	Damage potential: 10 Reproducibility: 7 Exploitability: 8 Affected users: 10 Discoverability: 8

Threat	MITM / server impersonation
Affected component	Authorization
Module details	?
Vulnerability class	?
Description	The protocol don’t require any type of certificate, and therefore the client don’t have any way to tell if he is getting responses from the server or from someone else who controls the communication. Attacker can use that fact to impersonate the server and establish communication with the client, leading to potentially sensitive information being sent to the attacker instead of the legitimate server.
Result	Client unknowingly sending his file to malicious server.
Prerequisites	Attacker have access to the communication channel & messages being sent to the server, either by interfering with the client traffic or the server traffic.
Business impact	Potentially sensitive data leaks.
Proposed remediation	Add certificate layer to the protocol.
Risk	Damage potential: 10 Reproducibility: 6 Exploitability: 3 Affected users: 5 Discoverability: 8

Threat	Identity theft
Affected component	Authorization
Module details	key exchange component
Vulnerability class	unauthorized access
Description	The protocol separates the name+id setting from public key exchange into two different messages. An attacker with read access to the clients messages can take the name+id and exchange his own public key with the server, acquiring full control on that user.
Result	Attacker steal the user (name+id) during creation
Prerequisites	Attacker has can communicate with the server, and listen to the messages the user gets.
Business impact	Attacker can pretend to be any legit user upon registration.
Proposed remediation	Merge name assignment and public key exchange into one stage and message
Risk	Damage potential: 5 Reproducibility: 6 Exploitability: 6 Affected users: 4 Discoverability: 10

Threat	Message replay
Affected component	File saving
Module details	File saving
Vulnerability class	?
Description	As long as the AES key don’t change, resending the same 1028-code messages would lead to the same result, moreover, file name is not protected so it can be changed, Allowing attacker that caught one 1028-code message to send it again and different file names and fill the users folder with unwanted copies of he’s file, potentially overriding other important files if implementation allowes.
Result	Attacker can store files for other users (with fixed content)
Prerequisites	Attacker has can communicate with the server, and can read at least one 1028-code message.
Business impact	Users folder is full of garbage.
Proposed remediation	include a digital signature of something that changes from one message to the other like current time or message index or server generated phrase.
Risk	Damage potential: 8 Reproducibility: 10 Exploitability: 8 Affected users: 8 Discoverability: 8