Hen Golubenko

Vulnerabilities Analysis

Threat	Server impersonation resulting in deceiving client to send personal information
Affected component	Authentication, Files
Vulnerability class	CWE-300: Channel Accessible by Non-Endpoint
Description	An attacker can pretend to be the host (man in the middle attack) and proxy all the information that the client sends to the server, and the server sends to the client. If the client thinks that the attacker is the true host, they might use the attacker's AES key and send them the secret files.
Result	Client might be deceived into connecting a malicious host and send sensitive information to it (like UUID and secret files).
Prerequisites	Attacker can connect to the network of the client and perform MITM attack (for example by ARP spoofing).
Business impact	Client's secret information is sent to a third party without their knowledge
Proposed remediation	Usage of certification in the server side and proper validation of it in the client side
Risk	Attack Vector (AV) – Network Attack Complexity (AC) – Low Privileges Required (PR) – None User Interaction (UI) – Required Scope (S) – Unchanged Confidentiality (C) – High Integrity (I) – High Availability (A) – None **Overall – 8.1 (high)**

Threat	Client is being impersonated
Affected component	Authentication, Files
Vulnerability class	CWE-319: Cleartext Transmission of Sensitive Information
Description	The UUID and the name of the client, which are the only information required for successful login, are transmitted cleartext, thus exposing the client to the threat of credentials theft and impersonation.
Result	Client's credentials being stolen, and someone uses them to login in, performing actions on behalf of their name (like exchanging keys and sending files). Possibly also **information exposure**, if the server sends an error when sending a file with a name that already exists in the client's folder, or **overriding client's information** if file with already existing name was sent and the server simply overrides the former file.
Prerequisites	It is possible to connect to the network and intercept the traffic.
Business impact	Possible loss of client's data and possible information exposure. Client's account may become inaccessible.
Proposed remediation	Encrypt all data transmitted like TSL.
Risk	Attack Vector (AV) – Network Attack Complexity (AC) – Low Privileges Required (PR) – None User Interaction (UI) – Required Scope (S) – Unchanged Confidentiality (C) – High Integrity (I) – High Availability (A) – High **Overall – 8.8 (high)**

Threat	Client is being impersonated
Affected component	Authentication
Vulnerability class	CWE-1391: Use of Weak Credentials
Description	Login is performed with UUID and name. UUID are "128 bits long and can guarantee uniqueness across space and time" (RFC 4122). There is no demand for using cryptographically secure PRNG, and the server may use statistical PRNG instead, which pose increased risk of an attacker guessing the UUID. The name is not secured at all and can be any text, short as it may be, and easy to know or guess. Moreover, the protocol states that the UUID and name should be stored in an unprotected file on the client's machine, which increases the chance of unauthorized attacker to get them.
Result	Same as previous.
Prerequisites	It is possible to connect to the network and intercept the traffic, or get the client's credentials file.
Business impact	Possible loss of client's data and possible information exposure. Client's account may become inaccessible.
Proposed remediation	Use stronger authentication system, that doesn't rely on users keeping their UUID in secret and doesn't rely on the UUID implementation to be secure (for example, OTP).
Risk	Attack Vector (AV) – Network Attack Complexity (AC) – Low Privileges Required (PR) – None User Interaction (UI) – Required Scope (S) – Unchanged Confidentiality (C) – High Integrity (I) – High Availability (A) – High **Overall – 8.8 (high)**

Threat	Server become inaccessible and crashes due to DoS or DDoS attacks
Affected component	All of the server functionality
Vulnerability class	CWE-400: Uncontrolled Resource Consumption
Description	The protocol doesn't include rate limiting or congestion control mechanisms, making it vulnerable to attacks that can overwhelm it with excessive traffic.
Result	DoS and DDoS can cause the server to become unresponsive or unavailable to legitimate users.
Prerequisites	Sending a large amount of requests is not blocked by the server
Business impact	Legitimate users can't use the server.
Proposed remediation	1. Usage of rate limiting mechanisms to restrict the number of requests or connections a client can make within a certain time frame. 2. Limit the number of concurrent connections, thus preventing an attacker from exhausting server resources by opening numerous connections simultaneously.
Risk	Attack Vector (AV) – Network Attack Complexity (AC) – Low Privileges Required (PR) – None User Interaction (UI) – None Scope (S) – Unchanged Confidentiality (C) – None Integrity (I) – None Availability (A) – High **Overall – 7.5 (high)**

Threat	Private key is compromised or tempered with
Affected component	Files
Vulnerability class	CWE-1125: Excessive Attack Surface
Description	The private key is stored both in priv.key and in me.info.
Result	This can result in inconsistencies, synchronization challenges and increased attack surface. Access to private key allows, combined with other attacks, to get the aes key of the legitimate user and perform actions on their behalf.
Prerequisites	Access to me.info or priv.key files, and having them unencrypted and unprotected
Business impact	User's secret information can be exposed to third party.
Proposed remediation	Store private key
Risk	Attack Vector (AV) – Network Attack Complexity (AC) – Low Privileges Required (PR) – None User Interaction (UI) – None Scope (S) – Unchanged Confidentiality (C) – None Integrity (I) – None Availability (A) – High **Overall – 7.5 (high)**