Vulnerability Report – Q1 protocol – MMN 15

Name: Gil Alpert

I.D: 328259809

Date of Assignment: 30.3.2023

1 Table of Contents

2 Overriding Files

Threat	Overriding files
Affected component	Files stored on the server
Vulnerability class	Data integrity
Description	Clients save their files on the server without identifying themselves. The only form of identification is the client encrypting the file when sending to the client. Given an existing client id and a given filename (which aren't encrypted), a potential attacker could send the server that file, identifying with the given id, with dummy file contents, and override the file saved on the server.
Result	Untrusted clients can delete other clients' files and get rid of all their saved data.
Business impact	A malicious user or third-party company can delete the data of all users, sabotaging the business completely.
Proposed remediation	Modify the protocol such that a user must send an encrypted password, set at registration time, with every file send operation.
Risk	Damage potential: 9 Reproducibility: 10 Exploitability: 7 Affected users: 10 Discoverability: 8 **Overall: 9.3**

3 Server Impersonation

Threat	Server Impersonation
Affected component	Entire system
Vulnerability class	Authentication and Impersonation
Description	The server and clients are vulnerable to a MITM style attack. A potential attacker who's able to take control of the communication infrastructure can receive the messages from the client, save the id, username, and filename, create an RSA pair of his own, and talk to the server himself (impersonating the client). The client will think they are responding to the server and vice versa. If that succeeds, the attacker could store anything he'd wish on the server. When the client comes to use the backup he though he made of his files, not only they wont be there, but the client will be deceived by the data planted by the attacker.
Result	Anyone able to access the communications infrastructure in a MITM manner can control the data saved on the server entirely and deceive clients.
Business impact	Clients can be deceived by frankly anyone, ruining their trust in the service and compromising data integrity.
Proposed remediation	Add some sort of authentication system to the protocol: MAC/password/signature scheme (E.g., ElGammal).
Risk	Damage potential: 9 Reproducibility: 10 Exploitability: 3 Affected users: 5 Discoverability: 6 **Overall: 8.1**

4 Server Attack

Threat	Server Attack
Affected component	Security of files on server
Vulnerability class	Data security
Description	If a malicious attacker gains access to the data stored on the server, they can view all the clients' data and maybe even modify it (depending on the nature of the attack). Files are stored as plaintext and therefore are easy to access for a possible attacker who can gain access to the server.
Result	All files saved on the server are not secure, and their contents couldn't be trusted (depending on the nature of the attack).
Business impact	Clients can be deceived by frankly anyone, ruining their trust in the service and compromising data integrity.
Proposed remediation	Store the files encrypted on the server and don't save the symmetric key, that way only the client will have access to the contents of the files.
Risk	Damage potential: 10 Reproducibility: 2 Exploitability: 1 Affected users: 5 Discoverability: 8 **Overall: 5.9**

5 Distributed Denial-of-Service (DDoS)

Threat	Distributed Denial-of-Service (DDoS)
Affected component	Server
Vulnerability class	Service availability
Description	An attacker could send many and many requests from different IP addresses to the server, sending files with a very big size repeatedly.
Result	The server will be busy processing the dummy files sent by the distributed systems and will overwhelm, having to the deny service of customers.
Business impact	Clients will not be able to send files or access their data (in case that its possible, which we assume is the key).
Proposed remediation	-
Risk	Damage potential: 5 Reproducibility: 6 Exploitability: 1 Affected users: 10 Discoverability: 7 **Overall: 3.8**