**Vulnerabilities Analysis**

Yehudit Yudelevich.

1.

|  |  |
| --- | --- |
| Impersonating another client | Threat |
| Validation and reliability of the system | Affected component |
| CWE-1391: Use of weak credentials | Vulnerability class |
| Using a unique identifier that is only 16 bytes long, which may be a focus for brute-forest attacks, trying to discover the identifier.  Also, the identifier is saved in the me.info file and an attacker may discover the file and thus discover the unique identifier, and impersonate another customer. | Description |
| Impersonating another client and performing actions on his behalf. | Result |
| network access. | Prerequisites |
| client information can be damaged, and data can disappear, and malicious data can be sent. | Business impact |
| Using a stronger unique identifier, with a greater strength of bits, that does not require saving in a file. | Proposed  remediation |
| Attack Vector (AV) - Network  Attack Complexity (AC) - Low  Required Privileges (PR) - None  User Interaction (UI) - Mandatory  Scope (S) - unchanged  Confidentiality (C) - high  Integrity (I) - high  Availability (A) - high  Total - 8.8 (high**)** | Risk |

2.

|  |  |
| --- | --- |
| DoS or DDoS attacks. | Threat |
| All functionality of the server, the server crashes. | Affected component |
| CWE-400: Uncontrolled Resource Consumption. | Vulnerability class |
| The protocol lacks rate limiting and congestion control mechanisms, which makes it susceptible to attacks that can flood it with excessive traffic. | Description |
| The server becomes unavailable. | Result |
| Sending a very large amount of requests at the same time. | Prerequisites |
| Inability of clients to access the server and receive service. | Business impact |
| 1: Implementing rate-limiting measures to control the number of requests or connections a client can initiate in a specified time period.  2: Limiting the number of simultaneous connections to prevent an attacker from draining server resources by creating multiple connections. | Proposed  remediation |
| Attack Vector (AV) - network  Attack Complexity (AC) - Low  Required Privileges (PR) - None  User interaction (UI) - none  Scope (S) - unchanged  Confidentiality (c) - None  Integrity (I) - None  Availability (A) - high  Total - 8 (high) | Risk |

3.

|  |  |
| --- | --- |
| Saving the private key in the file priv.key and me.info. | Threat |
| Clients’ information and details | Affected component |
| CWE-1125: Excessive attack surface. | Vulnerability class |
| The private key is stored in both the priv.key file and the me.info file, and an attacker may gain access and break into one of the files and thus obtain the private key. | Description |
| In combination with other attacks, an attacker may obtain the encrypted AES and once I have access to the files, he will be able to decrypt the encrypted key, and use it for his purposes. | Result |
| Gaining access to one of the two files where the private key is located. | Prerequisites |
| Sensitive client’s information can be disclosed to a third party. | Business impact |
| Encrypt both priv.key and me.info using strong encryption algorithms like AES, ensuring they are never stored in plaintext. Implement access control and password protection to limit unauthorized access. Regularly rotate and update encryption keys to maintain security over time. | Proposed  remediation |
| Attack Vector (AV) - network  Attack Complexity (AC) - Low  Required Privileges (PR) - None  User interaction (UI) - none  Scope (S) - unchanged  Confidentiality (c) - None  Integrity (I) - None  Availability (A) - high  Total - 8 (high) | Risk |

4

|  |  |
| --- | --- |
| Path Traversal | Threat |
| File handling system on the server side, which processes file paths provided by the client. | Affected component |
| CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | Vulnerability class |
| An attacker can exploit the file path input sent by the client to inject malicious file paths. This allows access to files outside the intended directory on the server. If the client sends a crafted path (e.g., using "../" to traverse directories), the server may attempt to open, delete, or manipulate critical system files that should not be accessible. | Description |
| This can lead to unauthorized file access, exposure of sensitive data, or modification and deletion of critical files on the server, potentially compromising the server’s integrity or availability. | Result |
| 1: The server accepts and processes file paths from the client without proper validation or sanitization.  2: The attacker has control over the file path sent to the server. | Prerequisites |
| Unauthorized access to sensitive files can lead to data breaches, manipulation of server configurations, and service downtime. This could result in financial losses, legal consequences, and reputational damage for the business. | Business impact |
| 1: Normalize and sanitize file paths received from the client to prevent directory traversal.  2: Implement strict access control mechanisms to ensure files are only accessed within the allowed directories.  3: Validate file paths against an allowlist of trusted directories. | Proposed  remediation |
| Attack Vector (AV) - Network Attack Complexity (AC) - Low Required Privileges (PR) - None User Interaction (UI) - None Scope (S) - Unchanged Confidentiality (C) - High Integrity (I) - High Availability (A) - High Total - 8.5 (High) | Risk |

5

|  |  |
| --- | --- |
| Race Condition in File Transfer | Threat |
| File transfer process between the client and server. | Affected component |
| CWE-362: Race Condition | Vulnerability class |
| During the file transfer process, there could be a timing vulnerability where multiple clients or processes attempt to modify the same file or resource simultaneously. This could result in incomplete or corrupted file transfers, or allow an attacker to manipulate the file being uploaded by another client. | Description |
| An attacker could exploit this condition to inject malicious content into a file being transferred, corrupting legitimate files, or preventing clients from successfully uploading or downloading files. | Result |
| 2: Multiple clients or processes attempt to access the same file or resource at the same time.  2: Lack of proper synchronization mechanisms in the file transfer system. | Prerequisites |
| File corruption or modification could result in loss of data integrity, operational disruptions, and increased vulnerability to further attacks. | Business impact |
| Implement proper synchronization mechanisms, such as file locks or atomic operations, to ensure that only one client or process can modify a file or resource at any given time. | Proposed  remediation |
| **Risk** **Attack Vector (AV)** - Network **Attack Complexity (AC)** - Medium **Required Privileges (PR)** - Low **User Interaction (UI)** - None **Scope (S)** - Unchanged **Confidentiality (C)** - Medium **Integrity (I)** - High **Availability (A)** - Medium **Total** - 7.0 (Medium) | Risk |

6.

|  |  |
| --- | --- |
| Insufficient Logging and Monitoring | Threat |
| Server-side logging and monitoring of client activity. | Affected component |
| CWE-778: Insufficient Logging | Vulnerability class |
| The system does not properly log or monitor critical events, such as file transfers, failed authentication attempts, or unusual client behavior. Without proper logging, it's difficult to detect unauthorized access, malicious activity, or operational issues. This leaves the system vulnerable to prolonged attacks without detection. | Description |
| Attackers can carry out malicious actions, such as unauthorized file transfers or tampering, without being detected. Additionally, incidents such as failed file uploads or suspicious requests may go unnoticed, hindering incident response efforts. | Result |
| 1: Lack of comprehensive logging for key events, such as file transfers and authentication attempts.  2: Absence of monitoring tools that can trigger alerts based on suspicious activity. | Prerequisites |
| The inability to detect and respond to attacks or operational failures in real-time could lead to data breaches, operational disruptions, and significant financial and reputational damage. Additionally, failure to log events might lead to non-compliance with security regulations. | Business impact |
| mplement robust logging mechanisms that track all critical activities (e.g., file transfers, login attempts, and abnormal client behavior). Ensure the logs are protected from tampering, and set up automated monitoring tools that can trigger alerts in case of suspicious activity. | Proposed  remediation |
| **Attack Vector (AV) -** Network **Attack Complexity (AC) -** Low **Required Privileges (PR) -** None **User Interaction (UI) -** None **Scope (S) -** Unchanged **Confidentiality (C) -** Medium **Integrity (I) -** Medium **Availability (A) -** Medium **Total** – 7.0 **(**Medium) | Risk |

Thank you very much for the course and good luck with the project review!