# 2022 LG Security Studio Project

## Vulnerability Information

| | |
|---|---|
| **Team** | 2 |
| **Author** | Woosuk Ahn |
| | Heewon Ahn |
| | Woosuk Jung |
| | Hyunmin Kim |
| | Jungsun Ko |
| | Hunjin Ha |
| **Date** | Jul. 5,  2022 |

## Vulnerability Information List

| Vuln Num. | Summary | Location | Consequences/ Impact | CVSS Score | Proof of Concept |
|---|---|---|---|---|---|
| 1 | **Information Disclosure**<br>When making a TLS connection with the Lookup server, only the server is authenticated, not mutual authentication, so if there is only RootCA, an attacker can access the Lookup server with a client created arbitrarily. | OpenALPR\studio\webapp\rootca.crt | Information disclosure (Attacker can receive vehicle information that he wants.) | Overall CVSS Score: **6.7** | 1. Write the Client TLS python code.<br>2. Use rootca.crt to connect Lookup server and TLS communication.<br>3. Enter the desired plateNumber.<br>4. Receive information.<br>See Vulnerability_1_testCode.py for the Client Python example code for Vulnerability validation. |
| 2 | **Elevation of Privilege**<br>*Access Control Policy:*<br>**- Admin :** can use all functionalities and make a new account<br>**- General User :** can use limited functionalities<br>We designed that ONLY “admin” has permission to make a new account.<br>“General User” has no | - Load the image under 1 x 1 size<br>- https://ahnlab2.lge.com:8000/login/signup/ and you can see the submit button. | If the attacker can get the user account temporarily anyhow (for example, bribe any police officer, or hacking or phishing), the attacker can make another user account and the attacker can use this new account to get the personal information from the plate number. | Overall CVSS Score: **6.3** | 1. Login to any General User Account.<br>2. Load image under 1 x 1 size<br>3.Access URL: https://ahnlab2.lge.com:8000/login/signup<br>4. The submit button is shown and a new account can be submitted even if General User.<br>5. Logout User and Login with New |

| Vuln Num. | Summary | Location | Consequences/ Impact | CVSS Score | Proof of Concept |
|---|---|---|---|---|---|
| | privilege to make a new account.<br>We have a validation mechanism for the uploaded image by checking the size of it. (if the upload image size is same as 1(width)x 1(height) or under)<br>If an exception occurs, we can see the submit button in the “New account” page.<br>we can access the New account link directly The general user also can see the link to create a new account and the user can make a new account. | | | | account.<br>6. Enroll device to the DUO for new userID and you can get the vehicle number by plate number image. *The first device enrolled in Duo becomes the primary authentication method. |
| 3 | **Spoofing**<br>ALPR System Email app password exposed in code and sending email using the email account. | webapp/Settings.py line 160 | The attacker can misuse this email address account. e.g.) The attacker sends spam using this account or other malicious email. The attacker send this | Overall CVSS Score: **7.5** | 1. Check the email password information(EMAIL_HOST_PASSWORD ) from code and the password information to PoC.<br>2. execute poc django server |

| Vuln Num. | Summary | Location | Consequences/ Impact | CVSS Score | Proof of Concept |
|---|---|---|---|---|---|
| | | | email to the police officer to lead them to a phishing site and get the login information, | | 3. browse http://127.0.0.1:8000/ in chrome.<br>4. send email (for spam or phishing)<br>Detail information is in Artifacts/PoC/03/poc_guide.txt |
| 4 | **Denial of Service**<br>When making a TLS connection with the Lookup server, only the server is authenticated , not mutual authentication, so if there is only RootCA, an attacker can access the Lookup server using a DoS attack. | Lookup server | **Denial of Service**<br>Client received a response message about 0.01 sec in normal. But After the DOS attack(40 malicious clients, each client sent about 500~ 600 per second), the client received a response message about 1 sec. It means the client can be slow about 20 times. | Overall CVSS Score: **4.3** | 1. Client send plate number to server<br>2. Attacker sends a large amount of malicious messages to the server<br>3. Server responses the message not only client but also attacker<br>4. Client received message slowly<br>5. print “OH !!!!” and stop video or occurred error CV::OutOfMemortError |
| 5 | **Information Disclosure**<br>If an attacker can get the passwd(key) used when encrypting Plate DB through reversing, an attacker can decrypt the DB and find the vehicle | **Plate DB File:** licenseplate.db (plateServer\x64\Release)<br>**The passwd is in the source code.**<br>- file: server.cpp | **Information disclosure**<br>An attacker can decrypt Plate DB and find all of the vehicle information from it. | Overall CVSS Score: **5.1** | 1. Reverse Engineering server.exe<br>2. Get password(key) used when encrypting Plate DB.<br>3. Make application to decrypting Plate DB with password(key) (Algorithm: AES-128, Rijndael/AES) |

| Vuln Num. | Summary | Location | Consequences/ Impact | CVSS Score | Proof of Concept |
|---|---|---|---|---|---|
| | information from it. | - line : 26<br>- password: **2Team_Ahnlab** | | | **PoC:** decryptPlateDB.exe |
| 6 | **Information Disclosure**<br>An attacker can access the Logging file and disclose sensitive information to its users. | **Logging application**<br>File : logging.txt (plateServer/x64/release) | **Information disclosure**<br>It is supposed to operate when a specific plate number is recognized. | Overall CVSS Score: **3.3** | 1. An attacker turns on live camera mode in the system.<br>2. The image of the LTM37 plate number is recognized in the system.<br>3. Client sends the specific plate number “LTM37” to the plate server.<br>4. Server writes private information to the logging.txt file.<br>5. An attacker can  see the information through the logging.txt file. |
| 7 | **Tampering, Denial of Service**<br>The configuration file of the lookup server is not encrypted. An attacker can access the configuration file and change values of the Max Client User and the Minimum Confidence | **Configuration File**<br>File: **server.config** (plateServer\x64\Release) | **Tampering, Denial of Service**<br>An attacker can change values of Configuration file<br>1.**Max Client User** (MaxClientNum)<br>If an attacker changes the value of | Overall CVSS Score: **4.8** | 1. Access server.config<br>2. Change values ‘Max Client User’ and ‘Confidence Level’ in the configuration file.<br>3. Execute server.exe |

| Vuln Num. | Summary | Location | Consequences/ Impact | CVSS Score | Proof of Concept |
|---|---|---|---|---|---|
| | Threshold for partial matching.<br>As a result, an attacker can make only the first plate information of the DB to be delivered and make it impossible for clients to access the Lookup Server anymore. | | MaxClientNum to 0, the client is no longer able to connect to the Lookup Server.<br>2.**Minimum Threshold** (MinThreshold) If an attacker changes the value of Minimum Confidence Threshold to 0,first vehicle information in the Plate DB is transmitted to the client without comparing whether the plate number matches. | | |
| 8 | **Denial of Service**<br>Web server connect plate server first. And send config information such as max user number and confidence level. Max user defined unsigned short (range is 0~ 65535). An attacker can attack using integer overflow. | **Web Access :** https://ahnlab2.lge.com:8000/alpr/config | **Denial of Service**<br>If the max user set to 0, the lookup server cannot service. | Overall CVSS Score: **4.4** | 1. An attacker connect to update configuration into the web page (/alrp/config)<br>2. An attacker put the 65536 value into the max_user input text box.<br>3. Web server sends the config message(max user = 65536)<br>4. The lookup server sets the max user to ‘0’. (integer overflow) |

| Vuln Num. | Summary | Location | Consequences/ Impact | CVSS Score | Proof of Concept |
|---|---|---|---|---|---|
| | | | | | 5. Normal client can not connect lookup server |
| 9 | **Spoofing, Tampering**<br>Using the unprotected server certificate and key, an attacker can create a malicious server and pretend to be a server to connect with the client.<br>An attacker can change the status of all vehicles to normal and send it to the client. | **Certificates:**<br>plateServer\RootCA\serverCrt.pem<br>plateServer\RootCA\serverKey.pem<br>(These certificates can be downloaded from our github.)<br>**Web Access:**<br>https://ahnlab2.lge.com:8000/alpr?value={attacker's lookup server IP address} | **Spoofing:**<br>**Tampering:**<br>Transmitting manipulated information.<br>As a result, a criminal can evade law enforcement or PII may be disclosed. | Overall CVSS Score: **6.7** | **Web browser :**<br>1. An attacker sends the server IP address to connect to its own fake lookup server.<br>The server's IP address can be sent using HTTP GET message.<br>**e.g.)**<br>**https://ahnlab2.lge.com:8000/alpr?value={attacker's lookup server IP address}**<br>2. After that, the web server connects to the attacker's lookup server.<br>**Make fake lookup server :**<br>1. Copy the unprotected server certificate and key.<br>2. Write the server TLS C++ code using the provided server code.<br>3. It pretends to be a server and induces a client to connect.<br>4. When a client connects, all |

| Vuln Num. | Summary | Location | Consequences/ Impact | CVSS Score | Proof of Concept |
|---|---|---|---|---|---|
| | | | | | Vehicle States are transmitted as Normal. (even if the vehicle is stolen) |
| 10 | **Denial of Service**<br>Specific image pattern will send a command to the server to perform a shutdown.<br>*Specific image pattern:* e.g.) “Ahnlab” comment is the jpeg image. Jpeg | malimage.jpg | Attacker upload specific signature jpeg image file, web server disconnect to lookupserver. So, the system cannot retrieve vehicle information | Overall CVSS Score: **4.2** | 1. Attackers make a fake image to perform a system control command.<br>2. Upload a fake image to the web server.<br>3. Web server is triggered to command a lookup server to be shutdown. |

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator