

DRM

Nedostatky kodu

- Nepouzite premenne
 - DataServerApp-Base.cpp; 142
 - DRM_Client-ICCard.cpp; 183
- Nepremazane kluce
 - DataServerApp-Base.cpp; napr. “encryption_key”
- Nedealokovana pamat
 - DataServerApp-Base.cpp; 190, 195...
- Slaba nahodnost generovania IV
 - srand((unsigned)time(0));

- `memcpy(unsignedMemblock, memblok, size)`
- literal miesto konstant
 - `aes_setkey_enc(&aes_enc_ctx, encryptKey, 128);`

`char* encryptionKey = new char;`

...

```
bool readEncryptionKey(char* &encryptionKey, ...){  
    encryptionKey = new char[size+1];}
```

- Nepremazanie klucov
 - LicenceServerApp-base.cpp; encryptionKey
- delete memblock; miesto []

```
secretContent = new  
    char[strlen(constSecretContent)];  
strcpy(secretContent,constSecretContent);
```

- mnoho rovnakych funkcií ala copy&paste -
napr. generateIV
- nie je dokumentácia
- dll knižnica sa vyhľadáva v celej PATH miesto
lokálne