

Obecné

- Přehledný, čistý kód
- Licenční server a klient nejsou implementované
- Celková velikost přes 300 MB

Datový server

Obecné chyby

soubor	číslo řádku	popis chyby
TDataServer.cpp	25	Nekontrolování výstupu funkce GenerateAESKey
TDataServer.cpp	40	Nekontrolování výstupu funkce EncryptDataAES128

Bezpečnostní chyby

Nebyly nalezeny.

Šifrování

Obecné chyby

soubor	číslo řádku	popis chyby
Cipher.cpp	146	Nekontroluje se spočítání hashe
Cipher.cpp	171	Nekontrolování výstupu funkce ReadRSA3072PublicKeyFromFile

Bezpečnostní chyby

Identifikace problému: C₁

Závažnost: Vysoká

Proveditelnost útoku: Neznámá

Popis problému:

Cipher.cpp:79,86,100:CryptDataAES128() – Po chybě se okamžitě opouští funkce. Nedojde k přepání paměti s citlivými informacemi.

Navrhované řešení: Vynechat vyskočení z funkce a pro provádění dalšího kódu testovat, jestli je proměnná status rovná 0 (tedy nenastala chyba).

Identifikace problému: C₂

Závažnost: Nízká

Proveditelnost útoku: Neznámá

Popis problému:

Cipher.cpp:46:getSHA512Hash() – Neuvolněný SHA4 kontext

Navrhované řešení: Přepsat paměť kontextu

Identifikace problému: C₃

Závažnost: Nízká

Proveditelnost útoku: Neznámá

Popis problému:

Cipher.cpp:150:SignDataWithRSA3072() – Po chybě se okamžitě opouští funkce. Nedojde k přepání paměti s citlivými informacemi.

Navrhované řešení: Vynechat vyskočení z funkce a pro provádění dalšího kódu testovat, jestli je proměnná status rovná 0 (tedy nenastala chyba).