

## **Obecné**

- Chybějící dokumentace architektury
- Chybějící knihovny polarssl
- Chybějící unit testy
- 200 MB na 6 \*.cpp souborů mi přijde hodně
- Žádný refactoring
- Velice špatná (téměř žádná) práce s uvolňováním paměti

## **Refactoring**

- 6 vnořených ifů
- cpp i h soubory rozkopírovány vícekrát (Base64)
- Nekonzistence komentářů s kódem (DataServer base.cpp main metoda)
- Vracení 1 jako true a 0 jako false (někde obráceně)
- Některé funkce berou okolo 10 parametrů
- Boolovský výraz lze použít i v returnu
- Místy opakující se kód
- Zbytečné proměnné (atributy třídy - Polar.cpp)
- Pojmenování souborů a funkcí (CamelCase, podtržítka)
- Zbytečné metody compareHashes (stačí použít memcmp)
- Doporučuji: <http://knihy.cpress.cz/cisty-kod.html> [Čistý kód, Robert C. Martin]

# DataServer

## Obecné chyby

soubor	číslo řádku	popis chyby
base.cpp	150	Vyskočení z programu s hodnotou -1
base.cpp	159	Nepoužití std::string.find()
base.cpp	xyz	Neuvolňování alokované paměti

## Bezpečnostní chyby

**Identifikace problému:** C<sub>1</sub>

**Závažnost:** Vysoká

**Proveditelnost útoku:** Není třeba, chyba v kódu

**Popis problému:** base.cpp:240:calculateBlockedSize - špatný výpočet (ceil)

**Navrhované řešení:** Zaokrouhlování nahoru

**Identifikace problému:** C<sub>2</sub>

**Závažnost:** Vysoká

**Proveditelnost útoku:** Těžko rozhodnout, ale 3x větší pravděpodobnost úspěchu

**Popis problému:** base.cpp:181-191:main - Klíče jsou do paměti ukládány 3x, mazány ani jednou

**Navrhované řešení:** Použít std::string.c\_str()

**Identifikace problému:** C<sub>3</sub>

**Závažnost:** Nízká

**Proveditelnost útoku:** Těžko rozhodnout

**Popis problému:** base.cpp:321:main - Zbytečnou dlouho otevřený vstupní soubor

**Navrhované řešení:** Zavřít hned po načtení potřebných dat

**Identifikace problému:** C<sub>4</sub>

**Závažnost:** Střední

**Proveditelnost útoku:** Vzhledem ke struktuře kódu se může stávat často

**Popis problému:** base.cpp:348:main - Hmac spočítán, ale do souboru uložen až po vykonání bloku kódu

**Navrhované řešení:** Zapsat hned po výpočtu

**Identifikace problému:** C<sub>5</sub>

**Závažnost:** Vysoká **Proveditelnost útoku:** Těžko rozhodnout

**Popis problému:** Polar.cpp:33:generateIV - Generování náhodných dat

pomocí `srandr`, `rand`

**Navrhované řešení:** PolarSSL má dobré funkce na generování náhodných dat

**Identifikace problému:** C<sub>6</sub>

**Závažnost:** Vysoká

**Proveditelnost útoku:** Těžko rozhodnout, ale 2x větší pravděpodobnost úspěchu

**Popis problému:** `Polar.cpp:41:encrypt` - Kódy jsou do paměti zkopírovány dvakrát, nepřemazány

**Identifikace problému:** C<sub>7</sub>

**Závažnost:** Nízká

**Proveditelnost útoku:** Těžko rozhodnout

**Popis problému:** `Polar.cpp::Polar` - Nepoužit GCM mód, ale HMAC

**Navrhované řešení:** PolarSSL `gcm.h`

# LicenseServer

## Obecné chyby

soubor	číslo řádku	popis chyby
base.cpp	181	Dvakrát alokované encryptionKey. Uvolněné?
base.cpp	184	Nesedí komentář
base.cpp	42	Délka vstupu a výsupu jsou daleko od sebe

## Bezpečnostní chyby

**Identifikace problému:** C<sub>8</sub>

**Závažnost:** Střední

**Proveditelnost útoku:** Těžko rozhodnout

**Popis problému:** base.cpp:197:outputGcmKeyToFile - Nejprve příprava dat, pak test otevření souboru

**Navrhované řešení:** Prohodit činnosti

**Identifikace problému:** C<sub>9</sub>

**Závažnost:** Vysoká

**Proveditelnost útoku:** Závisí na možnosti volat Public metody

**Popis problému:** LicenseService.cpp:90:prepareLicenseInfo - Public metoda, která ukládá do paměti data

**Navrhované řešení:** Skrýt ji jako private, kontrolovat vstup

**Identifikace problému:** C<sub>10</sub>

**Závažnost:** Vysoká

**Proveditelnost útoku:** Nástroj k útokům

**Popis problému:** LicenseService.cpp:138:outputXmlFile - 21x použit operátor new

**Navrhované řešení:** Použít 21x operátor delete