

Identifikace problému: A0: lze získat dešifrovaná data

Závažnost: vysoká

Proveditelnost útoku: snadná

Popis problému: útočník může serveru poslat vlastní klíč, ke kterému zná privátní část.

Navrhované řešení: podepsat veřejné klíče klientů kořenovým klíčem.

Identifikace problému: A1: lze obejít metriky přehrávání

Závažnost: vysoká

Proveditelnost útoku: snadná

Popis problému: metriky se ukládají jako součást zašifrovaného balíku. Útočník může balík nahradit původní verzí a tak metriky obejít.

Navrhované řešení: ukládat metriky na bezpečné místo (token).

Identifikace problému: C2: Lze přehrávat vlastní balíky pomocí licence určené jinému klientovi.

Závažnost: vysoká

Proveditelnost útoku: závisí na konkrétní binárce

Popis problému: Main.cpp:54 – Nekontroluje se úspěšnost dekrypce klíčů; balík je potom verifikován a dekryptován chybným (a předem známým) klíčem.

Navrhované řešení: Kontrolovat úspěšnost kryptografických operací.

Identifikace problému: C3: Při generování licence se nekontroluje validita veřejného klíče.

Závažnost: nízká

Proveditelnost útoku: nelze rozhodnout

Popis problému: Útočník může získat licenci s dopředu známým obsahem a podpisem serveru.

Navrhované řešení: Ověřit platnost klíče.

Identifikace problému: C4: Vygenerované klíče se ukládají chybně

Závažnost: vysoká

Popis problému: Licence[sic] server\Main.cpp:57: Soubor .kf se otevírá textově, data jsou tedy poškozená a generování balíků nefunguje.

Navrhované řešení: Otevírat soubor binárně.

Identifikace problému: C5: Generované klíče pro AES a HMAC mohou být korelované

Závažnost: nízká

Proveditelnost útoku: nelze rozhodnout

Popis problému: PRNG se před každým použitím seeduje znovu.

Navrhované řešení: seedovat PRNG pouze jednou.

Identifikace problému: C6: Klient při přehrávání zahodí konec souboru

Závažnost: vysoká

Popis problému: PackageParser.h:80:PackageParser::Play – výstupní proud je zkrácen o délku metadat.

Navrhované řešení: Opravit.

Identifikace problému: C7: Buffer overflow při přehrávání krátkých balíků

Závažnost: vysoká

Proveditelnost útoku: obtížně

Popis problému: PackageParser.h:87:PackageParser::Play – celý vstupní balík (včetně HMAC signatury) je načten za hranice bufferu.

Navrhované řešení: Opravit.

Identifikace problému: C8: Lze klientovi vnutit nepodepsanou licenci

Závažnost: nízká

Proveditelnost útoku: nízká

Popis problému: Main.cpp:42:main – Verifikace podpisu licence a načtení obsahu licence neprobíhá atomicky, obsah souboru lze nahradit.

Navrhované řešení: Otevřít soubor jen jednou

Identifikace problému: C9: Klient crashne při jakékoliv chybě

Závažnost: nízká

Proveditelnost útoku: nízká

Popis problému: PackageParser.h:56 – Destruktor se pokouší mazat přes neinicializovaný pointer.

Navrhované řešení: Nepoužívat dynamicky alokované membery.

Identifikace problému: C10: Používá se vlastní formát klíčů

Závažnost: nízká

Proveditelnost útoku: nízká

Popis problému: údržba kódu

Navrhované řešení: Používat standardní formát

Identifikace problému: A11: neexistuje dokumentace architektury

Závažnost: vysoká

Proveditelnost útoku: snadná

Popis problému: DoS: systém neexistuje

Navrhované řešení: napsat dokumentaci

- Děkuji za generátor klíčů a za inicializátor tokenu.
- Většinou je vhodné předávat parametry referencí, zejména pokud jsou typu std::string.
- Standard vyžaduje, aby soubory byly ukončené znakem nového řádku.
- Místo strlen/strcpy lze používat std::string.
- Nulování pole
 - `char zeros[AES_BLOCK] = {0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0};`
 - `char zeros[AES_BLOCK] = {};`
- 112 zbytečných new. (Vytvářet objekty automaticky.)
- (unsigned char *)pp.getAESkey().c_str() je UB, pro klíče je lepší použít std::vector