Penetrační testy desktopových aplikací

AEC

Uchovejte firemní údaje a data svých klientů v bezpečí

Ať již se jedná o krabicové řešení třetí strany nebo výsledek vlastního vývoje, bezpečnost je v případě desktopových aplikací zásadní, neboť obvykle mají přístup ke kritickým firemním datům. U Desktopových aplikací se nebojíme jít s pomocí dekompilace až na úroveň zdrojového kódu, včetně jeho úprav, s cílem identifikovat z pohledu bezpečnosti riziková místa, citlivá data nebo jiné nedostatky v autorizaci či samotném přenosu mezi klientskou aplikací a serverem.

www.aec.cz

Penetrační testy a audity:

Desktopových aplikací
Provádíme penetrační testy již kompilovaných binárních aplikací, psaných v libovolném jazyce vůči bezpečnostním standardům a doporučením napříč celou řadou oblastí, majících dopad na bezpečnost samotné aplikace a citlivých dat, se kterými pracuje.

Úroveň prověření je komplexní s cílem identifikovat slabá místa či přímé zranitelnosti. Oblasti, pokrývající bezpečnost desktopových aplikací lze zjednodušeně definovat následovně:

- chyby validace uživatelských vstupů,
- nedostatky v řízení přístupů,
- slabiny autentizace a session managementu,
- výskyt Buffer Overflow zranitelností,
- možnosti injektáže vlastního kódu,
- nedostatečně ošetřené chybové stavy,
- nedostatky v bezpečnosti ukládání a přenosu dat,
- zátěžové testy (Denial of Service),
- ostatní chyby konfiguračního charakteru.

Zdrojových kódů
Kontrolujeme zdrojové kódy aplikací a asistujeme našim zákazníkům při vývoji bezpečných aplikací.

Penetrační testy desktopových aplikací

Penetrační testy desktopových aplikací jsou ve srovnání s penetračními testy webových aplikací v mnoha ohledech poměrně specifické. Vyžadují komplexní znalosti jak z oblasti bezpečné autentizace, autorizace přístupů a práce s citlivými daty, tak i hluboké znalosti programovacích jazyků včetně assembleru, práce v dissambleru, debuggeru s přímým použitím kódů instrukční sady (tzv. opcodes).

Výsledkem je ověření, zda je aplikace bezpečná, vhodná pro produkční nasazení a netrpí žádnou zjevnou bezpečnostní slabinou, která by mohla představovat přímé bezpečnostní riziko jak pro samotnou aplikaci, její uživatele, tak samotná data.

Následuje podrobnější výčet oblastí, které bývají z pohledu bezpečnosti desktopových aplikací i na základě našich dlouholetých zkušeností, kritické. Uvedený výčet není kompletní, nicméně podává zřetelnější představu o rozsahu a komplexnosti penetračních testů desktopových aplikací, ať již se jedná o vlastní vyvíjené řešení nebo řešení třetí strany, které se chystáte do svého prostředí nasadit. Rádi vám s řešením bezpečnosti pomůžeme.

Kritické oblasti pro bezpečnost desktopových aplikací

- Aplikace ukládá citlivá data v nešifrované podobě
- Vytvořené soubory mají přiřazena vysoká přístupová práva
- Nedostatečná kontrola vstupů na straně serveru
- Zranitelnosti komunikační brány
- Možné DoS testy komunikačních bran
- Citlivé údaje jsou posílány přes nešifrovaný komunikační kanál
- SSL/TLS nedostatky (verze, algoritmy, délky klíčů, validita certifikátů)
- Je použit proprietární komunikační protokol
- Nedostatky vzájemné autentizace kanálu
- Dlouhé timeouty čekání na odpověď serveru
- Nedostatečná kontrola klientských vstupů
- Možnosti obejití autentizačního schématu
- Absence použití více faktorové autentizace
- Možnosti brute-force útoku na autentizační údaje
- Slabá politika hesel
- Spustitelné soubory nejsou podepsány
- Session tokeny nejsou generovány s dostatečnou entropií
- Dlouhé trvání uživatelské relace
- Absence automatického odhlášení při neaktivitě
- Citlivé informace ukládané v cache paměti
- Ukládání citlivých informací do log souborů
- Kryptografie použita při ukládání dat není bezpečná
- Spustitelný kód obsahuje citlivé údaje
- Citlivá business logika obsažena v programu
- Vývojářské komentáře v souborech programu
- Nejsou použity žádné obfuskátory kódu
- V paměti se nacházejí citlivá data
- Nedostatky business logiky aplikace

Analýzy zdrojových kódů

- Kombinace statické analýzy pomocí automatizovaných nástrojů a manuální revize kódu
- Jazyky JAVA, C#, případně jiné, na dotaz

Naše přednosti

- Patříme mezi zavedené české security firmy, na trhu úspěšně působíme již déle než 30 let.
- Máme více než 15 let zkušeností na poli bezpečnosti desktopových aplikací.
- Náš tým tvoří specialisté se zkušenostmi ze stovek dílčích projektů.
- Jsme držiteli certifikací eMAPT, CISSP, OSCP, OSCE, CEH a celé řady dalších.
- Provozujeme vlastní hackerskou laboratoř na výzkum v řadě oblastí, zabývajících se bezpečností různých řešení.
- Naslouchámě klientům a přizpůsobujeme testy jejich potřebám a časovým možnostem.
- Sledujeme moderní trendy v oblasti bezpečnosti desktopových aplikací.
- Při testování klademe důraz na manuální přístup, který vede k odhalení většího množství chyb zejména v business logice aplikací oproti automatizovaným nástrojům.

Praha – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283