FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Miroslav Prágl, MBA
Student:	Bc. Jakub Štrom
Název práce:	Windows Sandbox: Analýza a ověření známých zranitelností
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	3. června 2024

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

Samotné zadání je poměrně náročné, Windows Sandbox je relativně nová a spartánsky zdokumentovaná součást OS Windows. Jeho splnění vyžadovalo nadstandardní úsilí, studentem objevená dosud neznámá zranitelnost je toho důkazem.

2. Písemná část práce 95 / 100 (A)

Práce je dobře čitelná, věcně správná, vyvážená a přehledná. Již jen ucelený autorský popis funkčnosti Windows Sandbox a souvisejících subsystémů OS je hodnotným dílčím tématem, na které plynule a logicky navazují další části práce. Vzhledem k citlivosti nemohl autor v práci uveřejnit některé hodnotné důkazy (např. předběžně přidělené CVE číslo, pod kterým je nová zranitelnost vedena), oponent je ale obdržel.

3. Nepísemná část, přílohy 90 / 100 (A)

Součástí práce jsou i konkrétní use case a zdrojový kód, použitelné pro demonstraci nalezené zranitelnosti. Po rychlé konzultaci ohledně drobných nejasností v deklaracích / externích knihovnách se podařilo základní ověření konceptu.

4. Hodnocení výsledků, jejich využitelnost 100 / 100 (A)

Práce nejen že uceluje a doplňuje relativně málo známé informace, ale přináší i zcela nové poznatky.

Celkové hodnocení

95 /100 (A)

S chutí jsem si přečetl ucelené pojednání o Windows Sandbox, které se dívá hodně "pod kapotu". Nově nalezená a nahlášená zranitelnost je pak třešničkou na dortu, která dělá FITu čest .

Otázky k obhajobě

Firma Microsoft nedávno avizovala ukončení podpory Application Guard a doporučuje místo něj využití Windows Sandboxu. Můžete popsat nějaké scénáře použití Windows Sandbox v tomto kontextu?

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.