FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jiří Dostál, Ph.D.
Student:	Vojtěch Krejsa
Název práce:	Analýza zranitelnosti CVE-2022-37434 v knihovně Zlib
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	12. června 2023

Hodnotící kritéria

1. Splnění zadání

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

Zadání bylo splněno.

2. Písemná část práce 100 / 100 (A)

Rozsah práce je přiměřený vzhledem k obsahu, práce je vyvážená a logicky členěna. Jazykově je práce, až na pár drobností, v pořádku. Text je srozumitelný a konzistentní v celém rozsahu. Autor použil relevatní zdroje, bibliografické citace jsou v souladu s citačními zvyklostmi a normami.

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

Výsledkem je SW dílo - proof of concept aplikace a virtuální stroje demonstrující analýzu zranitelnosti knihovny Zlib.

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

Výsledkem práce je pěkná, vyčerpávající a detailní analýza zranitelnosti CVE-2022-37434 včetně praktického výzkumu chování a možností exploitace v operačních systémech Linux a Windows. Jelikož mnoho zranitelností v databázi CVE je pouze stručně popsáno, tato analýza nabízí nebývale detailní vhled do podstaty zranitelnosti a popisuje problémy jednotlivých platforem včetně počátečních podmínek a limitace exploitace.

Celkové hodnocení

100 /100 (A)

Práce je celkově na úrovni diplomové práce a vzhledem k výše uvedeným kritériím ji celkově hodnotím stupněm A - výborně a doporučuji k obhajobě.

Otázky k obhajobě

Co Vás vedlo k volbě analýzy zrovna této knihovny?
Jaké jsou možnosti ochrany proti této zranitelnosti bez zásahu do zdrojového kódu? Myšleno na úrovni HW/OS - jsou-li nějaké vůbec?

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.