FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš, Ph.D.
Student:	Jakub Ferjak
Název práce:	CVE-2023-37903: Zranitelnost vzdáleného spuštění kódu v knihovně vm2
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	1. 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

2. Písemná část práce 95 /100 (A)

Písemná část práce velmi přehledně a srozumitelně provádí čtenáře všemi aspekty vm2, které jsou potřeba pro porozumění analyzované zranitelnosti a jejím důsledkům. Text je výjimečně dobře napsaný s mnoha příklady, takže ani neznalý čtenář nebude mít pocit, že vůbec nechápe, o co jde. Ani po faktické stránce nenacházím žádné problémy, jazyková stránka je také v pořádku. Jediné dvě výtky mám k tomu, že kapitola Conclusion není uvedena v obsahu a že v listingu 2.1 je chybně použita funkce greet namísto správné hello. To jsou ale drobnosti.

3. Nepísemná část, přílohy 95 /100 (A)

Nepísemnou část práce tvoří demonstrační aplikace v Node.js, která přehledně demonstruje bezpečnostní problémy související s analyzovatelnou zranitelností, a to hned v několika různých sandboxovacích enginech. Součástí je také virtuální stroj, ve kterém je vše nainstalované a připravené, čtenáři stačí VM spustit a hned může zkoušet, zda jednotlivé techniky fungují. Podle mě jde přesně o to, co čtenář potřebuje.

4. Hodnocení výsledků, jejich využitelnost 85 /100 (B)

Dosažené výsledky přesvědčivě demonstrují, že analyzovatelná zranitelnost je velmi závažná a že je naprosto nutné přestat knihovnu vm2 používat co nejdříve. Z tohoto

pohledu je děsivé zjištění studenta, že i dnes, po téměř roce od zjištění zranitelnosti a ukončení vývoje knihovny, ji používají stovky balíčků a registruje skoro 2 miliony stažení týdně. Doufám, že i díky této práci by se pozorovaná čísla mohla snížit.

Práce nenabízí konkrétní úpravy v knihovně, protože jak student vysvětlil, celý koncept knihovny je od začátku problematický a problémy jsou do značné míry neřešitelné. Navíc existují alternativní knihovny, které tímto principiálním problémem netrpí.

5. Aktivita studenta

[1] výborná aktivita
[2] velmi dobrá aktivita
[3] průměrná aktivita
▸ **[4] slabší, ale ještě dostatečná aktivita**
[5] nedostatečná aktivita

Student pracoval převážně samostatně, bylo jen velmi málo konzultací.

6. Samostatnost studenta

▸ **[1] výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Celkové hodnocení 95 /100 (A)

Student provedl analýzu zranitelnosti CVE-2023-37903. Popsal její příčiny i důsledky a vytvořil server, který přesvědčivě ukazuje, proč je zranitelnost tak kritická. Provedl také analýzu dalších knihoven s obdobnou funkcionalitou a došel k závěru, že tyto obdobnou zranitelností netrpí a mohou posloužit jako vhodná alternativa pro projekty, které potřebují sandboxovací nástroj pro JavaScript. Podle mě nejpřínosnější částí práce je mimořádně přehledný a srozumitelný popis všech prvků, ze kterých zranitelnost vyplývá, který je použitelný obecně pro každého vývojáře v JavaScriptu a podle mě i pro každého zájemce o informační bezpečnost. Práci doporučuji k obhajobě a hodnotím známkou A-výborně.

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.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

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.