FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš, Ph.D.
Student:	Pavel Holý
Název práce:	Analýza zranitelnosti CVE-2023-4863 v knihovně libwebp
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	27. května 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 90 /100 (A)

V textová části práce provádí student čtenáře celou problematikou zranitelnosti CVE-2023-4863. Seznamuje ho stručně s problematikou přetečení bufferu a klíčovými částmi knihovny libwebp, aby následně mohl detailně analyzovat předmětnou zranitelnost a vysvětlit, jak přesně dochází k přepsání paměti mimo buffer a za jakých podmínek. Nakonec ukazuje, jak může útočník tyto znalosti použít k vytvoření exploitu, který spustí jím určený kód. Popis je dosti hutný, ale stále srozumitelný, bez faktických chyb. Po technické stránce též bez připomínek.

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

Nepísemnou část práce tvoří proof-of-concept (POC) spuštění kódu ve zranitelné aplikaci a virtuální stroj, který tuto zranitelnost umožní snadno vyzkoušet. Student za tímto účelem vytvořil vlastní aplikaci pro konverzi .webp obrázků do .png, což pro POC zcela vyhovuje - exploitování zranitelnosti ve skutečných aplikacích by bylo výrazně složitější a nemělo by žádné skutečné přínosy, jen rizika pro uživatele, kteří třeba ještě neaktualizovali své zranitelné verze. Z POC je mimo jiné poznat, že zneužití zranitelnosti není úplně přímočaré, je vyžadováno dosti specifické rozložení paměti, nicméně jak je vidět, je možné ho dosáhnout. Jedinou výhradu mám v tom, že popis použití je pouze v readme souboru, a to ještě jen pro základní variantu - pokud si uživatel chce udělat vlastní experiment, musí si potřebné informace, co kde a jak změnit, dohledat sám.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Dosažené výsledky přesvědčivě ukazují, že analyzovaná zranitelnost je aspoň potenciálně použitelná ke spuštění libovolného kódu čistě jen na základě vhodně upraveného obrázku. Vyžaduje sice specifické podmínky, takže dosáhnout takového zneužití s reálnými aplikacemi rozhodně není jednoduché, ale jednoznačně nám ukazuje, že takové zneužití možné je. Lze také snadno vyzkoušet, že i kdyby útočník nedokázal spustit svůj vlastní kód, učitě dokáže aplikaci shodit a tím dosáhnout odepření služby (denial-of-service). Toto vše by mělo být velmi přesvědčivým argumentem pro každého uživatele, aby okamžitě aktualizoval jak knihovnu, tak všechny aplikace, které ji využívají.

5. Aktivita studenta

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

Aktivita studenta byla slabší, proběhlo jen několik málo konzultací. Student je však zjevně nepotřeboval.

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 se velmi kvalitně zhostil svého úkolu. Analyzoval čerstvou zranitelnost a porozuměl jí do té míry, že byl schopen provést útok typu "remote code execution" za pomoci vhodně upraveného obrázku. Svá zjištění také přehledně popsal a připravil demonstrační prostředí pro vyzkoušení si takového útoku. Nebylo to jednoduché a skutečnost, že to student dokázal, bez pochyb ukazuje, že si zaslouží titul bakaláře v oboru informatika. Práci doporučuji k obhajobě a hodnotím 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.