Posudek diplomové práce

Matematicko-fyzikální fakulta Univerzity Karlovy

Autor práce	Václav Šraier		
Název práce	Performance of Open vSwitch-based Kubernetes Cluster in Pathological Cases		
Rok odevzdání	2023		
Studijní program	Informatika	**Studijní obor**	Programování a softwarové systémy

Autor posudku	Jiří Benc	**Role**	Vedoucí
Pracoviště	Katedra distribuovaných a spolehlivých systémů - externí pracovník		

Text posudku:

Práce zkoumá chování Kubernetes clusteru při generování neočekávaného síťového provozu z některého z kontejnerů. Cílem práce bylo nalézt sekvence paketů, které budou mít vliv na výkon clusteru jako takového s potenciálně bezpečnostními důsledky (DoS útoky). Touto problematikou se dosud žádná práce uceleně nezabývá.

Zvolena byla typická konfigurace Kuberenetes clusteru, kdy je jako virtuální switch používán Open vSwitch.

Autor práce se po zorientování v problematice zcela zaměřil na slabiny návrhu a implementace Open vSwitch. Zde bych měl výtku k opominutí dalších možných problematických komponent clusteru; nicméně uznávám, že rozsah práce by narostl příliš nad to, co lze spravedlivě požadovat po diplomové práci. Naopak oceňuji, že během výzkumu autor nepodlehl pokušení k vytržení Open vSwitche a jeho testování samostatně (čímž by práce ztratila na hodnotě), ale celá práce probíhala v prostředí Kubernetes. Pro tento účel vytvořil autor testovací software (cca 3000 řádků kódu), který je k práci přiložen.

Nejzajímavějšími výsledky práce jsou z mého pohledu identifikace sekvence paketů, kterou lze za určité softwarové nebo hardwarové konfigurace vyčerpat paměť Open vSwitch procesu a způsobit tak DoS útok na provoz ostatních uživatelů clusteru, a dále identifikace nedostatku v návrhu architektury Open vSwitch, kdy nelze efektivně vyjádřit pravidla pro firewall, která jsou typická pro prostředí Kubernetes. Tato neefektivita vede k vysokému nároku na výpočetní zdroje a má tak potenciál k umožnění či amplifikaci jiných útoků. Autor při výzkumu a analýze postupuje systematicky, lze se domnívat, že pro daný typ sekvencí (tedy sekvence zaměřující se na generování upcallů) identifikoval všechny relevantní problémy. Nezabývá se však otázkou, zda nelze generovat sekvence útočící na jiné aspekty Open vSwitche; očekával bych alespoň krátký rozbor tohoto tématu. Dále bych očekával rozbor bezpečnostních aspektů nalezených problémů.

Oceňuji, že autor nad rámec zadání zkoumal a potvrdil, že nalezené problémy lze reprodukovat i v odlišném nasazení Open vSwitch, konkrétně v OpenStack clusteru. Dále kladně hodnotím soubor doporučení pro provozovatele veřejných clusterů a návrhy vylepšení projektu Open vSwitch pro zmenšení důsledků nalezených problémů.

Po formální stránce je práce přehledná a dobře členěná. Vzhledem k problematice je

významná volba anglického jazyka. I přes gramatické a stylistické chyby hodnotím jazykovou úroveň práce jako vysokou.

Celkově práce přinesla zajímavé výsledky, je odborně a rozsahem na dobré úrovni a nedostatky uvedené výše nejsou zásadní. Práci doporučuji k obhajobě.

Práci doporučuji **k obhajobě.**

Práci nenavrhuji **na zvláštní ocenění.**

Datum 14. 8. 2023 **Podpis**