MINISTERSTVO ZEMĚDĚLSTVÍ

VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE Č. 1

Název veřejné zakázky:	**Systém pro správu zranitelností**
Druh zadávacího řízení:	Zjednodušené podlimitní řízení na služby dle § 53 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“ či „zákon“)
Zadavatel:	Česká republika – Ministerstvo zemědělství
Sídlem:	Těšnov 65/17, 110 00 Praha 1 – Nové Město
Zastoupený:	Bc. David Šetina, ředitel Odboru informačních a komunikačních technologií
IČO:	00020478
DIČ:	CZ00020478

Česká republika – Ministerstvo zemědělství jako zadavatel výše uvedené veřejné zakázky obdržel dne 7.12.2017 žádost o vysvětlení zadávacích podmínek. Níže uvádíme její úplné znění a odpověď zadavatele na položené otázky:

Otázka č. 1
Požadavek č. 14 je obecně plně splnitelný pouze s dodatečným software (v rozporu s požadavkem 1), takzvaným DAST. Řešení na management zranitelností obecně nepodporují aplikační skenování či podporuje pouze základní metody. Navrhujeme upravit na: Řešení musí podporovat základní možnosti skenování aplikací.

Odpověď zadavatele:
Zadavatel v tomto bodě požaduje testování zranitelnosti webových aplikací, které představují základní platformu pro poskytování většiny služeb zadavatele. OWASP TOP 10 je veřejně přijímaný dokument popisující aktuální zranitelnosti vyskytující se na této platformě. Požadavek na možnost testování těchto zranitelností je pro zadavatele zásadní. Základní možnosti skenování by dle našeho názoru měly zohledňovat minimálně zranitelnosti uvedené v dokumentu OWASP TOP 10. Rozpor s požadavkem č. 1 bude řešen úpravou jeho formulace tak, že nebude požadováno unikátní produktové pokrytí.

Otázka č. 2
Tento požadavek (č. 16) je mimo oblast řešení na vulnerability management. Požadavek je obecně splnitelný pouze s dodatečným software (v rozporu s požadavkem 1), takzvaným DAST. Navrhujeme požadavek vypustit.

Odpověď zadavatele:
Zadavatel uvedl požadavek na katalogizaci linků uvnitř webové aplikace v kontextu uživatele z důvodu snadnější orientace v její struktuře. Tento požadavek není s ohledem na identifikaci zranitelností relevantní. Zadavatel vypustí tento požadavek z technické specifikace VULN.

Otázka č. 3
Tento požadavek (č. 20) zcela mimo koncepci řešení na vulnerability management, která jsou bezpečná z pohledu provozu a zásadně neinvazivní. Požadavek lze splnit pouze speciálním software na penetrační testování. Navrhujeme požadavek vypustit.

Odpověď zadavatele:
Zadavatel uvedl požadavek na doplňkovou funkcionalitu s ohledem na vyhodnocení slabin v konkrétní oblasti bezpečnosti. Chápe však situaci, že ke zmíněnému cílení na danou oblast nemusí dojít jen prostřednictvím vyšší logiky funkcionality systému VULN, ale například analýzou výsledků nebo jejich statistickým vyhodnocením. Tento požadavek není s ohledem na identifikaci zranitelností zásadní a je možné ho realizovat v rámci dodávky služby jako celku. Zadavatel umožní realizovat tento požadavek i jinými prostředky (např. lidské zdroje).

Otázka č. 4
Řešení na management zranitelností obecně nepředpovídají zranitelnosti. Zranitelnost musí být nejdříve výrobcem přidána a řešení ji na základě této identifikace je schopno odhalit. Je samozřejmě schopné odhalit i potencionálně nebezpečné běžící služby. Navrhujeme požadavek (č. 32) vypustit.

Odpověď zadavatele:
Zadavatel uvedl požadavek na predikci „Zero-Day zranitelnosti“. Tím je myšleno, že zranitelnost kódu, která byla zveřejněna jeho výrobcem a na nějž neexistuje v době její identifikace v prostředí zadavatele opravná aktualizace, a nachází se tedy v intervalu WoV (Window of Vulnerability), bude predikována nebo jinak označena jako „čekající“. Při zveřejnění opravné aktualizace systém upozorní na takový patch bez návaznosti na sken zranitelnosti. Systém tedy sám upozorňuje na opravné aktualizace vztahující se ke známým zranitelnostem v prostředí zadavatele. Zadavatel v tomto smyslu přeformuluje požadavek.

Otázka č. 5
Zadavatel požaduje funkcionalitu vizualizace síťové topologie. Nástroje na management zranitelností nejsou z principu povahy své funkce (skenování na úrovni sítě) schopné informace o topologii získat. K tomu je nezbytný sběr konfiguračních dat z aktivních prvků a jejich vyhodnocení. Existují taková řešení na trhu nicméně jedná se o jinou kategorii řešení, než je Management zranitelností. Z důvodů požadavku na jednotný produkt je tento požadavek (č. 34) obecně nesplnitelný, prosíme o jeho odstranění.“

Odpověď zadavatele:
Zadavatel uvedl požadavek na vizualizaci z důvodu snadnější orientace v infrastruktuře zadavatele. Tento požadavek není s ohledem na identifikaci zranitelností, především formou služby, relevantní. Zadavatel vypustí tento požadavek z technické specifikace VULN.

Otázka č. 6
Řešení na management zranitelností obecně nepracují s pravděpodobností. Zranitelnost buď existuje nebo ne a je ohodnocena závažností. Navrhujeme požadavek (č. 35) vypustit.

Odpověď zadavatele:
Zadavatel v tomto bodě požaduje možnost vyfiltrovat z výsledku skenování aktiva dotčená novou zranitelností. Vyznačením pravděpodobnosti dopadu zranitelnosti je myšleno rovněž ohodnocení závažnosti. Jde tedy o možnost filtrovat položky tak, aby u jednotlivých záznamů nově dotčených aktiv byla vyznačena jejich závažnost.

Otázka č. 7
Požadavek (č. 51) je obecně splnitelný pouze s dodatečným software (v rozporu s požadavkem 1), takzvaným DAST. Řešení na management zranitelností obecně nepodporují aplikační skenování. Navrhujeme upravit na: Řešení musí podporovat základní možnosti skenování aplikací.

Odpověď zadavatele:
Zadavatel v tomto bodě požaduje reporting a filtrování výsledků testování zranitelnosti webových aplikací, které představují základní platformu pro poskytování většiny služeb zadavatele. OWASP TOP 10 je veřejně přijímaný dokument popisující aktuální zranitelnosti vyskytující se na této platformě. Požadavek na možnost reportování o těchto zranitelnostech je pro zadavatele zásadní. Rozpor s požadavkem č. 1 bude řešen úpravou jeho formulace tak, že nebude požadováno unikátní produktové pokrytí.

Zadavatel z důvodu potřebné změny ve specifikaci plnění a vysvětlení zadávací dokumentace, zveřejňuje upravenou technickou specifikaci (Příloha č. 5 Smlouvy) vztahující se ke službě „Systém pro správu zranitelností“ a prodlužuje lhůtu pro podání nabídek na 11. ledna 2018.

V Praze dne 8. 12. 2017

Mgr. Tomáš Koliba
Digitálně podepsal Mgr. Tomáš Koliba
Datum: 2017.12.08 15:37:21 +01'00'

Ministerstvo zemědělství
Mgr. Tomáš Koliba
Odbor pro veřejné zakázky