Vilniaus miesto savivaldybės administracijos saugumo spragų pranešimų programos „Bug Bounty“ konkurso nuostatų
3 priedas

SAUGUMO SPRAGŲ LYGIŲ IR PRIZŲ DYDŽIŲ LENTELĖ PAGAL PROGRAMOS PAKOPAS (TIER)

Šiame priede pateikiami saugumo spragų kritiškumo lygiai ir jiems taikomi prizų dydžiai pagal dviejų pakopų (TIER) programos finansavimo modelį. Kiekvienas gautas pranešimas yra vertinamas pagal jo sudėtingumą. Gavus saugumo spragos pranešimą jis nagrinėjamas Konkurso komisijoje, kuri įvertina gautą saugumo spragos pranešimą pagal nustatytus kriterijus ir jį priskiria konkrečiam spragos lygiui. Pagal Konkurso komisijos nustatytą ir saugumo spragai priskirtą lygį Konkurso dalyviui skiriamas lentelėje nustatyto dydžio prizas.

Spragos kritiškumo lygis	**Prizo suma (Eur)**		**Pažeidžiamumas (spraga)**
	TIER 1 (Savivaldybės Sistemos)	**TIER 2 (Savivaldybės įmonių Sistemos)**	
Išskirtinė *(angl. Exceptional)*	3000 €	2000 €	Kokybiškas, išsamus pranešimas, atskleidžiantis išskirtinį poveikį VMSA ir jos klientams; paprastai priskiriamas aukšto ar kritinio sudėtingumo lygmeniui *(angl. A quality report that shows exceptional impact to VMSA and it's customers, typically otherwise in high or critical severity category)*
Kritinė *(angl. Critical)*	2000 €	1000 €	Spragos, sukeliančios neatidėliotiną riziką VMSA Sistemoms ar vartotojų duomenims *(angl. Critical severity issues present a direct and immediate risk to a broad array of our users or to a VMS IS itself)*
			Nuotolinio kodo vykdymas *(angl. Remote Code Execution)*
			Savavališkas kodo ar komandos vykdymas mūsų produkcinės aplinkos serveryje *(angl. arbitrary code or command execution on a server in our production network)*
			SQL įskverbties ataka *(angl. SQL Injection)*
			SQL užklausos produkcinėje duomenų bazėje *(angl. SQL queries on a production database)*
			Autentifikavimo arba autorizacijos apėjimas *(angl. Authentication or Authorization Bypass)*
			Prisijungimo proceso, slaptažodžių arba 2-jų faktorių autorizacijos apėjimas *(angl. Bypassing the login process, either password or 2FA)*
			Prieiga prie jautrių vartotojų duomenų arba vidinių produkcinės aplinkos Sistemų *(angl. access to sensitive production user data or access to internal production systems)*

Didelė *(angl. High)*	1000 €	700 €	Lokalaus failo įterptis *(angl. Local File Inclusion)*
			Paskyros perėmimas *(angl. Account Takeover)*
			Masinis asmens identifikavimo informacijos išgavimas *(angl. Mass PII Extraction)*
			Horizontalus privilegijų eskalavimas klientų lygmenyje. Horizontalus privilegijų eskalavimas įvyksta tada, kai vartotojas įgyja kito vartotojo (turinčio tokį patį prieigos lygmenį, kaip ir jis) prieigos teises. *(angl. Horizontal Privilege Escalation across customer contexts; horizontal privilege escalation is when a user gains the access rights of another user who has the same access level as he or she does.)*
			Vertikalus privilegijų eskalavimas. Vertikalus privilegijų eskalavimas įvyksta tada, kai užpuolikas pasinaudoja Sistemos spraga, kad pasiektų daugiau nei jam leidžiama su turimomis vartotojo teisėmis. *(angl. Vertical Privilege Escalation; vertical privilege escalation is when an attacker uses a flaw in the system to gain access above what was intended for him or her)*
Vidutinė *(angl. Medium)*	300 €	200 €	Nesaugi tiesioginė objekto nuoroda *(angl. Insecure Direct Object Reference (IDOR)*
			Serverio užklausų klastojimas *(angl. Server-Side Request Forgery (SSRF)*
			XSS ataka, kai įterptas kodas „atsispindi“ Web aplikacijoje *(angl. Reflected Cross-Site Scripting)*
			Kelių svetainių scenarijų ataka (angl. Stored Cross-Site Scripting (XSS)) *(injecting attacker controlled content into *.vilnius.lt (XSS) that bypasses CSP)*
			Kryžminių svetainių užklausų klastojimas *(angl. Cross-Site Request Forgery (CSRF))*
			Jautrių duomenų išnaudojimas *(angl. Sensitive Data Exposure)*
			Nepageidaujamo (žalingo) kodo įterpimas *(angl. Cross-Site Script Inclusion (XSSI))*
Maža *(angl. Low)*	100 €	70 €	Masinis vartotojų išvardijimas, kurio metu surandamas validžių vartotojų sąrašas *(angl. Mass User Enumeration)*
			Dokumento objekto modelio (DOM) įterptinių komandų ataka *(angl. DOM-based Cross-Site Scripting)*
			Slaptažodžių perdavimas atviru tekstu (HTTP protokolu)

			(angl. Clear text Submission of Passwords (over HTTP))
			Pažeidžiamumas, kuris leidžia valdyti peradresavimą arba atlikti nukreipimą į kitą URL adresą. *(angl. Open Redirect)*
			Ataka, kuri leidžia užpuolikui įterpti HTML kodą į tinklalapius, kuriuos mato kiti vartotojai (angl. HTML content injection)
			Nebegaliojančių ar pasenusių nuorodų perėmimas *(angl. Broken Link Hijacking)*
			PHP informacijos atskleidimas *(angl. PHP Info Disclosure)*
			Autentifikavimo galinių taškų greičio apribojimo problemos *(angl. Rate limit issues on authentication endpoints)*
			Pateiktas pranešimas kuria pridėtinę vertę ir pateikia informaciją apie kurią prieš tai nebuvo žinoma *(angl.Created Additional Value)*
Nenagrinėtinas pagal Konkurso nuostatas (atmetamas kaip neatitinkantis sąlygų)	Prizas neskiriamas	Prizas neskiriamas	Pranešimas pateiktas pasibaigus nustatytam pranešimų pateikimo terminui
			Pranešimą pateikė asmuo, negalintis dalyvauti konkurse
			Pranešimas pateiktas kitu, nei nuostatuose nustatytu būdu (nesant pagrįstų priežasčių, paprastai nepriklausančių nuo pačio dalyvio)
			Išnaudotos konkursui skirtos lėšos einamiesiems metams
			Dalyvis nesusipažino su konkurso sąlygomis ir nepasirašė konfidencialumo pasižadėjimo
			VMSA turi duomenų, kad Dalyvis neatitinka konkurso reikalavimų
			Nepagrįstas pranešimas (spragos nėra arba ji nėra pripažinta keliančia grėsmę informacijos ar duomenų saugumui)
			Nepateiktas scenarijus, kaip atkartoti pažeidimą
			Nepateiktas argumentuotas paaiškinimas, kas gal nutikti nepašalinus atsiradusios spragos
			Pranešimas pateiktas apie Sistemą ar kitą IT išteklių, kuris neįeina į konkurso apimtį