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)

1. Spragų kritiškumo vertinimo principai

Šiame priede pateikiami saugumo spragų kritiškumo lygiai ir jiems taikomi prizų dydžiai pagal dviejų pakopų (TIER) finansavimo modelį. Gavus pranešimą apie saugumo spragą, jis nagrinėjamas Konkurso komisijoje, kuri, vadovaudamasi šiame priede nustatytais kriterijais, priskiria spragai konkretų kritiškumo lygį. Pagal nustatytą kritiškumo lygį Konkurso dalyviui skiriamas lentelėje nurodytas prizas.

Spragos kritiškumo lygis ir atitinkamas prizo dydis nustatomi atsižvelgiant ne tik į spragos tipą ar techninę klasifikaciją, bet ir į realų jos poveikį Konkurso organizatoriaus aplinkai. Vertinant realų spragos poveikį:

- ✓ spraga laikoma **išskirtinio**, **kritinio arba aukšto kritiškumo**, jei sudaro galimybę pasiekti kitų naudotojų jautrius duomenis, vykdyti privilegijuotus veiksmus arba reikšmingai paveikti Sistemos saugumą ar veikimą;
- ✓ spraga laikoma **vidutinio kritiškumo**, jei leidžia pasiekti ribotos apimties ar mažo jautrumo duomenis arba turi ribotą poveikį Sistemos funkcionalumui;
- ✓ spraga laikoma **žemo kritiškumo**, jei jos poveikis yra minimalus ir nesudaromos realios piktnaudžiavimo galimybės.

Spragos kritiškumo lygis nustatomas įvertinus šių veiksnių visumą:

- galimą poveikį duomenų konfidencialumui, vientisumui ir prieinamumui;
- spragos išnaudojimo sudėtingumą;
- realų išnaudojimo scenarijų ir praktinę galimybę jį įgyvendinti;
- paveiktų naudotojų ar sistemų mastą;
- ar spraga susijusi su vartotojų duomenų naudojimu ar tvarkymu;
- ar Sistema yra aktyviai naudojama produkcinėje aplinkoje;
- ar spraga sukelia realią ir reikšmingą riziką informacinei sistemai, įskaitant galimą poveikį Sistemos veikimui;
- kontekstinius veiksnius, tokius kaip autentifikacija, autorizacija, vieša ar ribota prieiga, integracijos su kitomis sistemomis ir pan.

Tais atvejais, kai spraga formaliai atitinka kritinio ar aukšto kritiškumo pažeidžiamumo požymius (pvz., *Remote Code Execution*, *Authentication Bypass* ar kt.), tačiau dėl Sistemos konteksto nesukelia realios saugumo rizikos ar faktinio poveikio, spraga gali būti priskirta žemesniam kritiškumo lygiui.

Vertinant spragas, prioritetas teikiamas realiam poveikiui, galimai žalai ir faktinei rizikai, o ne vien teoriniam ar techniniam spragos tipui. Komisija pasilieka teisę nustatyti galutinį spragos kritiškumo lygį, neatsižvelgdama į automatinę ar Konkurso dalyvio nurodytą spragos klasifikaciją (pagal 2 skyriaus prizų lentelę), ir atitinkamai skirti mažesnio dydžio prizą.

2. Prizų lentelė

Spragos kritiškumo lygis	Prizo suma (Eur)		Pažeidžiamumo tipas (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*)
Aukšto kritiškumo (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*)
Vidutinio kritiškumo (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)*)
Žemo kritiškumo (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*)

3. Pranešimai, kuriems prizas neskiriamas ir kurie nėra nagrinėjami

3.1. Prizas neskiriamas ir pranešimas nenagrinėjamas pagal Konkurso nuostatas (atmetamas kaip neatitinkantis sąlygų), jeigu nustatoma bent viena iš šių aplinkybių:

3.1.1. Pranešimas pateiktas pasibaigus nustatytam pranešimų pateikimo terminui.

3.1.2. Pranešimą pateikė asmuo, neturintis teisės dalyvauti Konkurse.

3.1.3. Pranešimas pateiktas kitu, nei Konkurso nuostatuose nustatytu būdu, kai nėra pagrįstų, nuo Konkurso dalyvio nepriklausančių priežasčių.

3.1.4. Išnaudotos Konkursui einamiesiems metams skirtos lėšos.

3.1.5. Konkurso dalyvis nesusipažino su Konkurso sąlygomis ir nepasirašė konfidencialumo pasižadėjimo.

3.1.6. Konkurso organizatorius turi duomenų, kad Konkurso dalyvis neatitinka Konkurso nuostatų reikalavimų.

3.1.7. Pateiktas nepagrįstas pranešimas (spraga nepasitvirtino arba nekelia grėsmės informacijos ar duomenų saugumui).

3.1.8. Nepateiktas spragos išnaudojimo (atkūrimo) scenarijus (*proof of concept*).

3.1.9. Pranešimas grindžiamas tik automatinių įrankių rezultatais, nepateikiant realaus spragos išnaudojimo demonstravimo.

3.1.10. Nepateiktas argumentuotas paaiškinimas dėl galimo poveikio ar žalos nepašalinus spragos.

3.1.11. Pranešimas pateiktas apie Sistemą ar kitą IT išteklį, kuris neįtrauktas į Konkurso apimtį.

3.2. Pranešimai apie saugumo spragas, kurios nustatomos ne Konkurso organizatoriaus valdomose ar kontroliuojamose Sistemose (Savivaldybės įmonių), o trečiųjų šalių sistemose, į kurias Konkurso organizatoriaus Sistema tik nukreipia vartotoją (*redirect*) ir kurių Konkurso organizatorius nekontroliuoja, laikomi nepatenkančiais į Konkurso apimtį (*out of scope*).

Tokiais atvejais Konkurso organizatorius vertina tik paties nukreipimo mechanizmo saugumą Konkurso organizatoriaus Sistemoje (pvz., ar nėra galimybės manipuliuoti nukreipimu, atlikti atviro peradresavimo ar kitų panašių pažeidžiamumų).

Spragos, kurios yra susijusios tik su trečiųjų šalių sistemų veikimu, konfigūracija ar saugumu, pagal Konkursą nėra atlyginamos.

3.3. Pranešimai apie duomenų pasiekiamumą nelaikomi saugumo spraga ir nėra atlyginami, jeigu nustatoma, kad:

- duomenys pagal Sistemos paskirtį, funkcionalumą ar galiojančius teisės aktus yra teisėtai ir sąmoningai viešai prieinami visiems vartotojams;
- duomenys tapo prieinami dėl vartotojo veiksmų ar žmogiškosios klaidos (pvz., vartotojo įkeltų ar paviešintų duomenų), o ne dėl Sistemos saugumo trūkumų.

Tokiais atvejais duomenų pasiekiamumas nėra laikomas Konkurso organizatoriaus Sistemos saugumo spraga, todėl piniginis prizas neskiriamas.

3.4. Spragos Sistemoje ar jos dalyje, kuri yra valdoma trečiųjų šalių sprendimu arba atvirojo kodo (*open source*) programine įranga (pvz., *API Gateway – Gravitee*), vertinamos atsižvelgiant į tai, ar jos:

- jau buvo viešai žinomos (pvz., paskelbtos *open source* bendruomenėje, CVE duomenų bazėje ar kituose viešuose šaltiniuose);
- turi realų ir patvirtinamą poveikį Konkurse dalyvaujančioms Sistemoms ar jose tvarkomiems duomenims.

Prizas skiriamas tik tuo atveju, kai:

- nustatomas tiesioginis ir reikšmingas poveikis Konkurso organizatoriaus aplinkai;
- Konkurso dalyvis pats užregistruoja spragą pas atitinkamos trečiosios šalies (pvz., *Gravitee* platformos) kūrėjus ar palaikytojus ir pateikia tai patvirtinančius įrodymus (pvz., registruoto pranešimo nuorodą, identifikatorių, ekrano nuotrauką ar kitą oficialų patvirtinimą).

Pranešimai apie spragas, kurios neturi realaus poveikio Konkurso organizatoriaus naudojamoms Sistemoms, laikomi nepatenkančiais į Konkurso apimtį (*out of scope*).