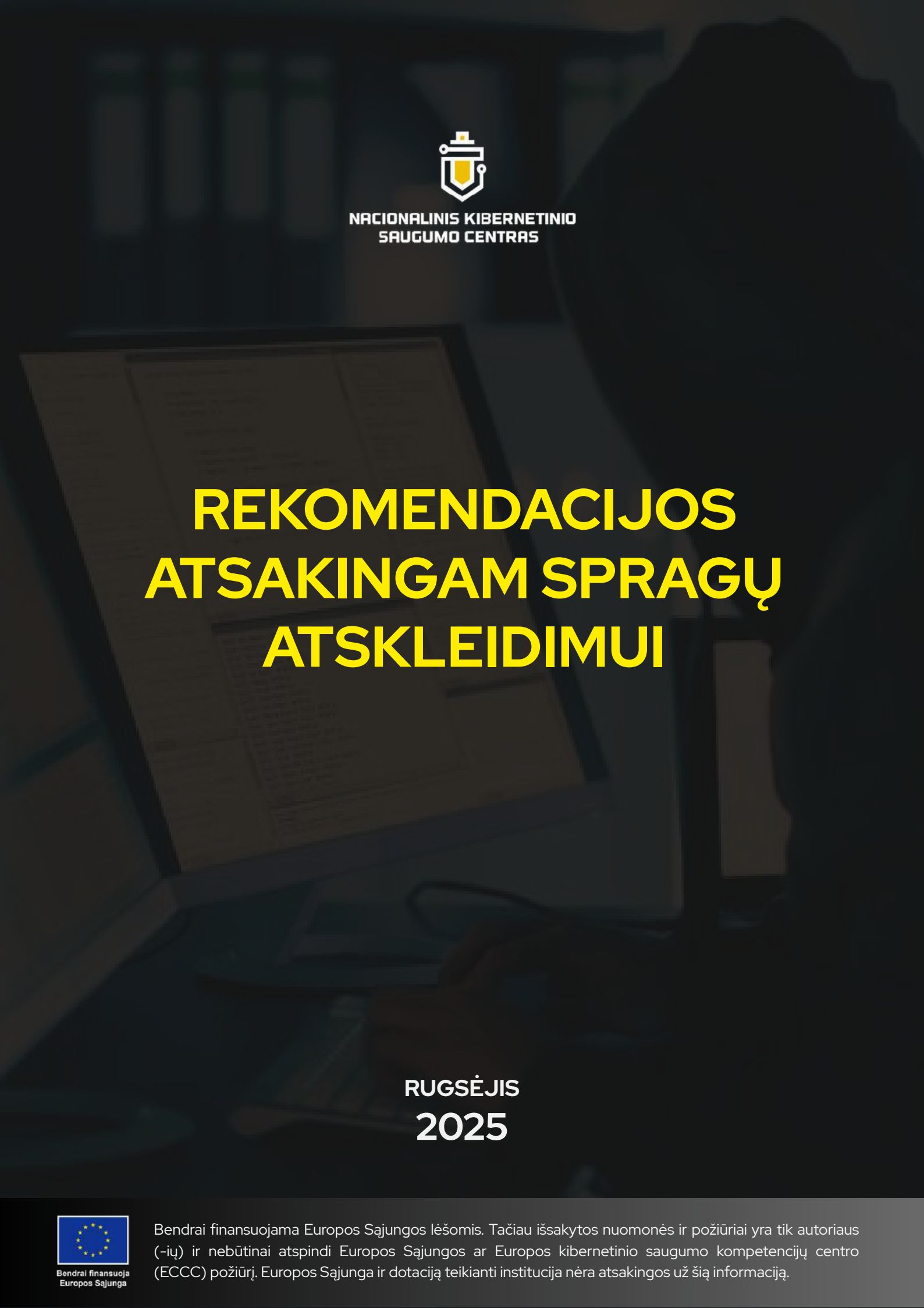


NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

REKOMENDACIJOS ATSAKINGAM SPRAGŲ ATSKLEIDIMUI

RUGSĖJIS
2025

Bendrai finansuoja Europos Sąjunga

Bendrai finansuojama Europos Sąjungos lėšomis. Tačiau išsakytos nuomonės ir požiūriai yra tik autoriaus (-ių) ir nebūtinai atspindi Europos Sąjungos ar Europos kibernetinio saugumo kompetencijų centro (ECCC) požiūrį. Europos Sąjunga ir dotaciją teikianti institucija nėra atsakingos už šią informaciją.

Turinys

NKSC rekomendacija

ATSAKINGAM SPRAGŲ ATSKLEIDIMUI

Šios rekomendacijos skirtos paaiškinti, kaip saugiai ir atsakingai atlikti pažeidžiamumų paiešką ir kaip tinkamai pranešti apie rastas kibernetinio saugumo spragas paveiktoms organizacijoms arba Nacionaliniam kibernetinio saugumo centrui (NKSC).

Auditorija

Informacija aktuali tiek patyrusiems programuotojams bei etiškiems įsilaužėliams, tiek ir asmenims, neturintiems specialių informacinių technologijų (IT) žinių, tačiau atsitiktinai aptikusiems galimą spragą.

Problematika

Atsakingas atskleidimas tampa vis svarbesne kiekvienos valstybės kibernetinio saugumo dalimi. Naujos spragos sistemose yra aptinkamos kasdien. Spragas pirmieji gali aptikti ne tik etiškieji įsilaužėliai, bet ir priešiškų valstybių tarnybos ar pelno siekiantys piktavaliai, todėl svarbu, kad ne tik profesionalūs etiškieji įsilaužėliai, bet ir pilietiški gyventojai bei organizacijos aktyviai prisidėtų prie spragų identifikavimo ir atskleidimo.

KAIP IEŠKOTI?

Lietuva buvo viena iš pirmųjų šalių pasaulyje, kuri įteisino atsakingą spragų atskleidimą. Kibernetinio saugumo įstatyme (KSĮ) buvo nustatytos ir taisyklės, kaip teisėtai ieškoti spragų. Svarbu laikytis šių taisyklių, kad nebūtų peržengtos teisinės ribos.

Netrikdyk sistemų darbo.
Negali būti trikdomas ar keičiamas sistemos darbas, funkcionalumas, teikiamos paslaugos ir duomenys.

Aptikęs spragą, sustok.
Įsitikinęs, kad spraga yra, nutrauk tolimesnę spragų paieškos veiklą.

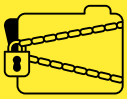
Pranešk kuo greičiau.
Apie vykdomą paiešką ir nustatytas spragas turi pranešti NKSC ir paveiktai organizacijai ne vėliau kaip per 24 valandas nuo paieškos pradžios.

Neperženk būtinumo ribos.
Atlik tik tiek veiksmų, kiek yra būtina spragos egzistavimui patvirtinti.

Neatskleisk asmens duomenų.
Atskleisdamas spragą viešai, neviešink jokių aptiktų asmens duomenų.

Nespėliok slaptažodžių.
Nebandyk atspėti slaptažodžių ir nenaudok neteisėtai gautų slaptažodžių.

Nenaudok socialinės inžinerijos.
Nebandyk išvilioti duomenų iš organizacijos darbuotojų socialinės inžinerijos metodais (pvz., phishing ar kt.).



Nesidalink su kitais.
Apie aptiktą spragą atskleisti viešai galėsi po 90 dienų. Per tą laiką kooperuok su NKSC bei paveikta organizacija ją šalinant bei informaciją apie spragą pasilaikyk tik sau.

Vykdant spragų paiešką, privaloma naudoti tik saugius paieškos metodus. Pirmenybė turėtų būti teikiama rankiniam ir pasyviam testavimui, kurio metu potencialus nepageidaujamas poveikis testuojamai sistemai yra minimalus. Naudojant automatizuotus įrankius, reikėtų rinktis pasyvius (angl. *passive / non-intrusive*) sprendimus. Labai svarbu tinkamai išsiaiškinti ir naudoti tik saugius įrankių parametrus, kad nebūtų generuojamas perteklinis užklausų kiekis ir nebūtų trikdoma sistema.

APIE KURIAS SPRAGAS PRANEŠTI ?

Spragų paieškos metu **dėmesys turėtų būti skiriamas spragoms, kurios kelia realią grėsmę sistemų ar jose saugomų duomenų saugumui.** Tai yra spragos, kurios leidžia apeiti taikomas saugos priemones, pasiekti ar pakeisti privačius duomenis, sutrikdyti sistemų veikimą ir pan. Pavyzdžiui:

- **SQL injection**
- **Remote code execution**
- **Netinkamos prieigos kontrolės priemonės**
- **Privačių duomenų prieiga dėl klaidingos konfigūracijos**

Dažniausiai aptinkamos spragos, kurios realios grėsmės nekelia. NKSC prašo nesiųsti informacijos apie spragas, jeigu jų išnaudoti kenkėjiškiems tikslams neįmanoma, pavyzdžiui:

- XSS tipo spragos statinėse svetainėse
- Atviri prievadai, kurių atvira prieiga nekelia grėsmės
- HTTP saugumo antraščių (angl. headers) trūkumas
- Identifikuojamos pasenusios programinės įrangos versijos, kurių išnaudojimas sistemoje neįmanomas
- Žinomos spragos (CVE), kurioms išnaudoti būtini specifiniai nustatymai, bet sistemoje jų nėra.

KAIP PRANEŠTI?

Apie nustatytą spragą gali pranešti sistemos valdytojui tiesiogiai, naudodamasis viešai pateiktais kontaktais arba jų pačių nurodytais būdais. Jeigu sistemos valdytojo nustatyti negali arba nusprendei pranešti NKSC, tuomet gali tai padaryti dviem būdais:

El. pašto adresu: **cert@nksc.lt** (jeigu informaciją teiksi šifruotu pranešimu, naudok NKSC viešąjį raktą: 0x3956D9B5).

Užpildydamas atsakingo atskleidimo formą NKSC interneto svetainėje: https://www.nksc.lt/pranesti-spraga.html

NKSC, gavęs pranešimą apie potencialią spragą, atlieka šios informacijos patikrinimą. **Užtenka pateikti tiek informacijos, kad būtų įmanoma identifikuoti spragą,** bet kuo išsamiau ir daugiau pateiksi informacijos, tuo lengviau bus patvirtinti pažeidžiamumo egzistavimą.

Esminiai duomenys:

- Sistema, kurioje vykdyta spragų paieška – pavadinimas, URL / IP adresas, prievadas
- Konkreti pažeidžiama vieta.

Papildomi duomenys:

- Data ir laikas.
- Papildoma techninė informacija, reikalinga atkartoti spragos išnaudojimą, t. y. konkretūs žingsniai, kaip buvo atrasta spraga.
- Kita informacija, galinti padėti identifikuoti spragą ir jos išnaudojimą (pavyzdžiui, ekrano vaizdai, vaizdo įrašas, naudoti įrankiai ir kt.).
- Tikėtinos pasekmės, jeigu spraga būtų pasinaudota (pavyzdžiui, perimti / sunaikinti duomenys, sutrikdyta sistema ir pan.).
- Kitos sistemos, produktai, organizacijos, vartotojai, kurie gali būti paveikti šios spragos.

VIEŠAS ATSKLEIDIMAS

Viešai atskleisti informaciją apie nustatytą spragą (pvz., savo tinklaraštyje ar soc. tinklo puslapyje) galima tik po 90 kalendorinių dienų nuo pirmo pranešimo išsiuntimo paveiktai organizacijai arba NKSC. Tam tikrais atvejais laikotarpis gali būti sutrumpintas:

NKSC sprendimu, kuomet informacija turi būti paviešinta greičiau, pavyzdžiui, kai apie spragą yra būtina kuo greičiau informuoti visuomenę.

Jei nustatyta, kad spraga nėra pavojinga arba subjektas, kurio sistemoje pastebėta spraga, raštu sutinka, kad informacija būtų paskelbta anksčiau.

Viešas atskleidimas yra galimas tik pagal nustatytą tvarką, su kuria galite susipažinti atnaujintame Nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos apraše.

NKSC dėkoja visiems pilietiškiems asmenims, kurie praneša apie spragas pagal atsakingo atskleidimo principus, jūsų pranešimai prisideda prie šalies kibernetinio saugumo stiprinimo. Aktyvus visuomenės dalyvavimas šioje veikloje yra svarbus veiksnys didinant šalies kibernetinį atsparumą.

ATSAKINGAS SPRAGOS ATSKLEIDIMAS

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Atsakingas spragų atskleidimas yra būtinas kibernetiniam saugumui užtikrinti, nes jas gali aptikti tiek etiški įsilaužėliai, tiek piktavaliai, todėl svarbu, kad prie identifikavimo prisidėtų ir pilietiški gyventojai bei organizacijos.

KAIP IEŠKOTI ?

Netrikdykite sistemų darbo.	Nedarykite įtakos sistemų darbui, funkcijoms ar duomenims.
Aptikę spragą, sustokite.	Patvirtinę spragą, nutraukite tolesnę paiešką.
Praneškite kuo greičiau.	Informuokite NKSC ir organizaciją per 24 val. nuo paieškos pradžios.
Neperženkite būtinumo ribos.	Darykite tik tiek, kiek reikia spragai patvirtinti.
Neatskleiskite asmens duomenų.	Atskleisdamas spragą, neskelbkite jokių asmens duomenų.
Nespėliokite slaptažodžių.	Nenaudokite spėjimo ar neteisėtai gautų slaptažodžių.
Nenaudokite socialinės inžinerijos.	Nenaudokite apgaulės ar manipuliacijos duomenims gauti.
Nesidalinkite su kitais.	Spragą viešinkite tik po 90 d., iki tol bendradarbiaukite tik su NKSC ir organizacija.

APIE KURIAS SPRAGAS PRANEŠTI ?

Spragų paieškos metu dėmesys turėtų būti skiriamas spragoms, kurios kelia realią grėsmę sistemų ar jose saugomų duomenų saugumui.

- **SQL injection**
- **Remote code execution**
- **Netinkamos prieigos kontrolės priemonės**
- **Privačių duomenų prieiga dėl klaidingos konfigūracijos**

KAIP PRANEŠTI?

El. paštu — cert@nksc.lt (jeigu informaciją teiksite šifruotu pranešimu, naudok NKSC viešąjį raktą: 0x3956D9B5);

NKSC interneto svetainėje — Užpildydami atsakingo atskleidimo formą NKSC interneto svetainėje: https://www.nksc.lt/pranesti-spraga.html

Viešai atskleisti spragą galima tik po 90 dienų nuo pranešimo paveiktai organizacijai ar NKSC, nebent NKSC arba organizacija sutinka anksčiau. Viešas atskleidimas galimas tik pagal Nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašą.

Bendrai finansuoja Europos Sąjunga

Bendrai finansuojama Europos Sąjungos lėšomis. Tačiau išsakytos nuomonės ir požiūriai yra tik autoriaus (-ių) ir nebūtinai atspindi Europos Sąjungos ar Europos kibernetinio saugumo kompetencijų centro (ECCC) požiūrį. Europos Sąjunga ir dotaciją teikianti institucija nėra atsakingos už šią informaciją.