КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 16 травня 2023 р. № 497

Київ

Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

Відповідно до пункту 2 розділу II "Прикінцеві положення" Закону України "Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану" Кабінет Міністрів України **постановляє:**

Затвердити Порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, що додається.

Прем'єр-міністр України **Д. ШМИГАЛЬ**

Інд. 49

- Порядок, що додається:
- P0497.doc.p/s

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 16 травня 2023 р. № 497

ПОРЯДОК
пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

1. Цей Порядок визначає механізм здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (далі — пошук потенційної вразливості системи).

Дія цього Порядку не поширюється на інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі, в яких обробляється службова інформація та/або інформація, що становить державну таємницю, розвідувальну таємницю, банківську таємницю.

2. У цьому Порядку терміни вживаються в такому значенні:

власник системи — фізична або юридична особа, якій належить право власності на систему;

вразливість системи — властивість системи, через використання якої створюється загроза для її безпеки, порушується сталий, надійний та штатний режим функціонування системи, здійснюється несанкціоноване втручання в її роботу, створюється загроза для безпеки (захищеності) електронних інформаційних ресурсів, конфіденційності, цілісності, доступності таких ресурсів;

декомпіляція — перетворення комп’ютерної програми з об’єктного коду у вихідний текст;

дизасемблювання — перетворення двійкового коду комп’ютерної програми в доступну для читання людиною форму;

дослідник потенційної вразливості (далі — дослідник) — фізична або юридична особа, яка здійснює пошук потенційної вразливості системи відповідно до вимог цього Порядку;

звіт про вразливість системи за результатами пошуку її потенційної вразливості (далі — звіт) — інформація про вразливість системи, підготовлена дослідником за результатами здійснення ним пошуку її потенційної вразливості;

зворотний інжиніринг — процес аналізу системи для ідентифікації її компонентів і визначення завдань, які вони виконують у системі;

зміни до системи — зміни, внесені до інформаційної (автоматизованої), електронної комунікаційної, інформаційно-комунікаційної системи, електронної комунікаційної мереж (далі — система) для вирішення проблеми вразливості системи, запобігання використанню вразливості, мінімізації можливих наслідків її використання;

координатор пошуку потенційної вразливості системи (далі — координатор) — фізична або юридична особа, яка надає послуги з організації пошуку потенційної вразливості системи;

період нерозголошення інформації про вразливість системи — строк, під час якого інформація про виявлену дослідником потенційну вразливість системи не підлягає розголошенню дослідником.

Інші терміни вживаються у значенні, наведеному в Законах України "Про основні засади забезпечення кібербезпеки України", "Про електронні комунікації", "Про захист інформації в інформаційно-комунікаційних системах", Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 р. № 518 (Офіційний вісник України, 2019 р., № 50, ст. 1697), ДСТУ ISO/IEC 29147:2016 "Інформаційні технології. Методи захисту. Розкриття вразливостей", ДСТУ ISO/IEC 27000:2015 "Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник".

3. Організація пошуку потенційної вразливості системи здійснюється її власником.

У разі потреби власник системи може прийняти рішення про залучення координатора для організації пошуку потенційної вразливості системи.

Залучення координатора відбувається шляхом укладення між власником системи та координатором договору про надання послуг з організації пошуку потенційної вразливості системи, в якому, зокрема, визначаються:

права та обов'язки, питання щодо платності чи безоплатності надання послуг з організації пошуку потенційної вразливості системи;

порядок та умови виплати винагороди досліднику, якщо така винагорода передбачена публічною пропозицією про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (далі — публічна пропозиція);

порядок звітування координатора перед власником системи про виплату винагороди досліднику, якщо така винагорода передбачена публічною пропозицією;

механізм інформування координатором власника системи про отриманий звіт і результати його перевірки;

механізм інформування власником системи координатора про результати перевірки звіту та прийняте рішення про внесення або невнесення змін до системи з урахуванням виявленої вразливості.

У разі коли договір про надання послуг з організації пошуку потенційної вразливості системи передбачає надання координатором платних послуг, такий договір укладається відповідно до вимог законодавства у сфері публічних закупівель.

4. Пошук потенційної вразливості системи здійснюється на підставі публічної пропозиції.

Публічна пропозиція оприлюднюється власником системи на власному офіційному веб-сайті.

У разі залучення власником системи координатора публічна пропозиція оприлюднюється координатором на його власному офіційному веб-сайті. У такому разі власник системи оприлюднює на своєму офіційному веб-сайті посилання на відповідну сторінку веб-сайта координатора.

Публічна пропозиція викладається українською мовою, при цьому додатково власник системи або координатор може викласти пропозицію іноземною мовою, яка є офіційною мовою Ради Європи.

5. Публічна пропозиція розробляється власником системи або координатором відповідно до примірної публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж і методичних рекомендацій з розроблення публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, що затверджуються Адміністрацією Держспецзв’язку.

6. У публічній пропозиції визначаються, зокрема:

інформація про систему, пошук потенційної вразливості якої здійснюється;

дії дослідника щодо системи, які йому заборонено проводити;

порядок надання дослідником звіту, вимоги до його підготовки, форми;

розмір, форма, порядок і умови виплати винагороди досліднику, який надав звіт, за результатами розгляду якого власник системи прийняв рішення про внесення змін до системи, та/або публічне висловлювання подяки;

період нерозголошення інформації про вразливість системи, що становить не більше шести місяців з дати реєстрації звіту.

Власник системи або координатор може визначити додаткові умови до публічної пропозиції з урахуванням секторальної (галузевої) специфіки функціонування системи.

7. Під час пошуку потенційної вразливості системи дослідник може:

здійснювати збір інформації про систему та умови її використання у відкритих джерелах;

аналізувати та вивчати документацію щодо роботи системи, оприлюднену власником системи або власником прав інтелектуальної власності на систему;

здійснювати збір публічно доступних даних про інфраструктуру та інтерфейси системи, сканувати мережу, хости і сервіси без подолання систем логічного захисту;

використовувати системи за призначенням і здійснювати нагляд за функціонуванням системи без порушення штатного режиму функціонування;

аналізувати алгоритми штатного режиму функціонування системи, порядок та результати виконання нею завдань, здійснювати пошук ознак поширеної вразливості системи, виявленої в інших системах;

здійснювати зворотний інжиніринг, декомпіляцію, дизасемблювання, відтворення системи в тестовому середовищі, модифікацію системи з метою пошуку її вразливості та проводити інші дії за згодою власника системи та власника прав інтелектуальної власності на систему та її компоненти, крім випадків, передбачених статтею 24 Закону України “Про авторське право і суміжні права”.

8. Після завершення пошуку потенційної вразливості системи дослідник повідомляє про результати власнику системи або координатору згідно з умовами публічної пропозиції та подає йому звіт.

9. Після отримання звіту власник системи або координатор протягом 10 робочих днів повідомляє досліднику про те, що звіт отримано, і зазначає його реєстраційний номер та дату реєстрації.

10. Власник системи та/або координатор перевіряє отриманий звіт на відповідність вимогам, визначеним публічною пропозицією, предмет наявності в ньому інформації про вразливість системи, виявлену раніше іншими дослідниками, вивчає умови та можливі ризики використання виявленої вразливості.

За результатами перевірки звіту власник системи оцінює можливі наслідки використання вразливості системи для її безпеки, порушення сталого, надійного та штатного режиму її функціонування, здійснення

несанкціонованого втручання в її роботу, створення загрози для безпеки (захищеності) електронних інформаційних ресурсів, конфіденційності, цілісності, доступності таких ресурсів (далі — наслідки вразливості системи) та приймає рішення щодо внесення або невнесення змін до системи.

За результатами перевірки звіту власник системи або координатор повідомляє про виявлену вразливість, щодо якої прийнято рішення про внесення змін до системи, урядовій команді реагування на комп'ютерні надзвичайні події України CERT-UA, а в разі наявності — галузевій команді реагування на комп'ютерні надзвичайні події. Власник системи, в якій обробляються державні інформаційні ресурси, оператор критичної інфраструктури повідомляє також Національній поліції та СБУ.

Після перевірки звіту власник системи або координатор протягом 30 робочих днів з дати реєстрації такого звіту повідомляє дослідникy про прийняте рішення щодо внесення або невнесення змін до системи.

У разі отримання від власника системи або координатора повідомлення щодо невнесення змін до системи дослідник має право оприлюднити інформацію про виявлену вразливість та її технічні особливості.

11. У разі прийняття рішення про внесення змін до системи власник системи вживає заходів щодо:

запобігання можливим наслідкам у разі використання вразливості;

внесення змін до системи.

Під час вжиття заходів щодо внесення змін до системи власник системи або координатор готує та оприлюднює інформацію про виявлення вразливості та внесення змін до системи, зокрема:

назву системи, її версію та іншу інформацію, яка дає можливість визначити систему, що містить вразливість;

дату виявлення вразливості;

опис вразливості;

реєстраційний номер звіту;

про користувачів, на яких могли вплинути наслідки у разі використання вразливості;

можливі наслідки, якщо такою вразливістю скористатися;

технічні особливості та інструкції щодо користування системою після внесення змін до системи.

Власник системи може прийняти рішення про оприлюднення інформації про виявлену вразливість до внесення змін до системи.

Якщо публічною пропозицією передбачено публічне висловлювання подяки, власник системи або координатор публікує повідомлення з висловленням подяки досліднику, в якому зазначається власне ім’я та прізвище або псевдонім дослідника (за його згодою).