Оцінка критичності вразливостей в операційних системах

Карина Ревізорова[1], Тетяна Гріненко[2]

1. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м. Харків, пр. Науки, 14, E-mail: karinamaroon71@gmail.com

2. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м. Харків, пр. Науки, 14, E-mail: tetiana.grinenko@nure.ua

Коротка анотація – Analysis of the vulnerability problem in operating systems. Comparison of existing vulnerability criticality assessment techniques. Review of existing software solutions in the global market. Sample metrics to assess vulnerability criticality.

Ключові слова – Вразливість, загроза, оцінка критичності вразливості.

I. Вступ

Одним з важливих заходів захисту інформації в комп'ютерних системах є визначення переліку загроз інформації. Загроза – можлива причина небажаного інциденту, який може завдати шкоди системі або організації [1]. Одна або декілька загроз можуть використовувати ряд вразливостей інформації. Вразливість в інформаційних технологіях (ІТ) – недолік або слабке місце, яке може бути використане для реалізації загрози [2]. Причинами виникнення вразливостей можуть бути помилки при проектуванні та в період розробки програмного (програмно-апаратного) забезпечення, неправомірна зміна режимів роботи пристроїв і програм або збої в їх роботі. Вразливість слід оцінювати, розглядаючи всі загрози, які можуть використовувати її у конкретній ситуації. Наслідками реалізації атаки на інформацію за допомогою вразливостей є: несанкціоноване розкриття, модифікація, пошкодження, знищення, недоступність або втрата інформації [2].

Вразливість, з моменту її виявлення і до випуску патча, має назву «вразливість нульового дня». Програма з такою вразливістю може бути зламана в будь-який момент, і відомості про такі вразливості так само є товаром. Після закриття вразливості (випуску патча) цінність вразливості падає. Вразливість, яка не має відповідної загрози, може не вимагати патчів, але розробники повинні її враховувати і піддавати моніторингу на предмет змін. Слід зазначити, що невірно реалізований або неправильно функціонуючий засіб контролю теж може бути вразливістю [2].

Більшість хакерських атак стають можливими через наявність вразливостей в існуючих операційних системах (ОС). ОС є найважливішим програмним компонентом будь-якої обчислювальної машини, тому від рівня реалізації політики безпеки в кожній конкретній ОС залежить і загальна безпека інформаційної системи [3]. Загрози безпеки ОС істотно залежать від умов експлуатації системи та від інформації, що зберігається і обробляється в системі, тощо. Наприклад, якщо ОС використовується для організації електронного документообігу, найбільш небезпечними є загрози, що пов'язані з порушенням цілісності та доступності інформації [4].

II. Засоби оцінки критичності вразливостей

Існує ряд систем оцінки вразливостей, які створені комерційними та некомерційними організаціями, наприклад, CERT/CC, система аналізу вразливостей SANS, система оцінки від Microsoft, CVSS, тощо [3].

Кожна з систем має свої переваги, але всі вони відрізняються за ознакою вимірювання. Наприклад, CERT/CC використовує значення оцінок від 0 до 180 і враховує такі фактори: чи схильна Інтернет-інфраструктура до ризику та який тип передумов потрібен для експлуатації вразливості. Система аналізу вразливостей SANS враховує: в якій конфігурації знайдена вразливість (стандартній чи ні), чи є система клієнтом або сервером [5]. Система оцінки від Microsoft намагається відобразити складність експлуатації та загальний вплив від експлуатації вразливості. Ці системи оцінки є корисними, але вони представляють підхід, при якому вважається, що наслідки експлуатації вразливості однакові для приватної особи і для компанії [5].

В результаті аналізу ринку програм з аналізу рівня критичності вразливостей, були виділені три продукти:

– PT Exploit Explorer (безкоштовна). Плюси: можливість завантажувати текстові файли; має корисні посилання на експлоіти. Мінуси: джерело для утіліти – база даних вразливостей CVE, яка дає мало інформації для оцінки; застосування тільки для вразливостей, для яких є експлоіти; неявно описано, яким чином здійснюється оцінка критичності вразливостей [5].;

– калькулятор CVSS V2 (безкоштовна). Плюси: детальний огляд метрик, за якими здійснюється оцінка. Мінуси: інтуїтивно незрозумілі критерії відбору; суперечлива логіка оцінювання;

– Nessus Vulnerability Scanner (обмежена free версія). Плюси: містить актуальні моделі загроз, на можливість експлуатації яких сканер швидко перевіряє клієнтську мережу. Мінуси: демонструє критичність вразливостей, тільки знайдених при скануванні [5].

III. Вибір метрик для оцінки критичності вразливостей

Кількісна оцінка безпеки має різні галузі. В залежності від того, як розглядати систему, метрики, що використовуються для оцінки критичності вразливостей можуть відрізнятися. Потрібно обирати метрики, які є практичними, корисними і значущими.

На підставі аналізу були вибрані наступні метрики впливу вразливостей, що дозволяють зловмиснику:

–впливати на конфіденційність (є влив/ не визначено);

–впливати на цілісність (є влив/ не визначено);

–впливати на доступність (є влив/ не визначено);

–дії направлені на пошкодження пам'яті (використовується/ не визначено);

–підбір паролів (використовується/ не визначено);

–спричинення до відмови в обслуговуванні (є влив/ не визначено);

–несанкціонована зміна прав доступу (використовується/ не визначено);

–злонамірне виконання довільного коду (використовується/ не визначено).

Також перевірка на:

–необхідність автентифікації для реалізації атаки (легко/ не визначено);

–складність експлуатації вразливості (легко/ не визначено);

–локальна або зовнішня взаємодія (локальна/зовнішня/ не визначено).

Ці метрики були вибрані на підставі аналізу опису вразливостей у ОС Windows за останні три місяці у БД вразливостей NVD.

IV. Аналіз вибраних метрик та порівняння оцінок

Щоб уникнути великої розбіжності результатів, була вибрана шкала від 0 до 10 та умовні позначення Low, Medium, High та Critical. Для кожного параметра вибраних метрик на основі експертної оцінки та порівняння показників у калькуляторі CVSS були виставлені коефіцієнти, в залежності має чи ні (чи не відомо) вразливість вплив на конфіденційність, цілісність, доступність, пошкодження пам’яті, та ін. Також на результат впливають вагові коефіцієнти складності експлуатації вразливості, чи є необхідність автентифікації для реалізації атаки та тип взаємодії (локальна, зовнішня чи не визначено).

Для порівняння у табл. 1 наведені результати розрахунків, які надає БД NVD, та розрахунки, що отримані на підставі вибраних метрик та вагових коефіцієнтів (у табл. 1 позначається як «*»).

ТАБЛИЦЯ 1

РЕЗУЛЬТАТИ РОЗРАХУНКІВ

Id	CVSSv3	Nvd.nist.gov	*
CVE-2018-4127	8,8	6,8	8,1
CVE-2017-7172	7,8	9,3	9
CVE-2018-6251	7,2	7,8	7,5

На підставі первинного аналізу (більше 100 вразливостей), відмінність між показниками CVSSv3 та Nvd.nist.gov становить 12,6%, а відмінність між CVSSv3 та «*» – 10,1% та між Nvd.nist.gov та «*» – лише 2,5%, можна зробити висновок, що параметри та коефіцієнти для оцінки були вибрані оптимально.

Висновок

Оцінка критичності вразливостей складний і суперечний процес, який складається з великої системи метрик, параметрів та експертних оцінок. Проведений аналіз методик оцінки критичності вразливостей існуючих програмних рішень на світовому ринку показав, що на даний момент не існує програмного забезпечення, яке могло б: аналізувати вразливості без допоміжних втручань користувача; аналізувати не тільки вразливості, для яких існують експлоіти; демонструвати вибірку вразливостей для кількох ОС у зручному форматі; проводити інтеграцію з базою даних вразливостей NVD (більш інформативною ніж CVE).

Резюмуючи вказане у другому розділі, обґрунтовано вимоги до методики оцінки вразливості:

–можливість оцінки ступеня ризику вразливості в залежності від можливості її експлуатації;

–результатом застосування методики має бути числове значення, що підходить для використання при аналізі ризиків;

–методика повинна мати можливість адаптації до конкретної інформаційної системи;

–параметри, які використовуються при розрахунку, повинні допускати мінімум різночитань;

–механізм розрахунку результуючого значення має бути простий і зрозумілий.

Враховуючи ці критерії, була розроблена методика, яка була взята за основу для розробки програмного продукту, що дозволить більш якісно і інформативно проводити оцінку критичності вразливостей.

Література

[1] ISO/IEC 27000 Информационные технологии - Методы и средства обеспечения безопасности - Системы менеджмента информационной безопасности – Общие сведения и словарь [Електроний ресурс] // ISO/IEC – 20.10.2019. Режим доступу: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27000-2016.pdf.

[2] Модель угроз ПД. Организационно-распорядительная документация по защите ПД [Електроний ресурс] // Институт.ру – Режим доступу: http://www.intuit.ru/studies/courses/ 697/553/lecture/12447 = 20.10.2019.

[3] Безбогов А.А. Безопасность операционных систем : учебное пособие / А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. – М.:"Издательство Машиностроение-1", 2007. – 220 с.

[4] Проблемы обеспечения безопасности ОС [Електроний ресурс] // Your Private Network. Режим доступу: http://ypn.ru/301/operating-systems-security-problems/- 31.10.2019.

[5] Полное руководство по общему стандарту оценки уязвимостей [Електроний ресурс] // securitylab. Режим доступу: https://www.securitylab.ru/ analytics/355336.php; - 31.10.2019.