УДК 681.04: 004.415.53 DOI: 10.26565/2519-2310-2022-2-04

# ОГЛЯД ПОТОЧНОГО СТАНУ ЗАГРОЗ, ЩО ОБУМОВЛЕНІ ВПЛИВОМ ЕКСПЛОЙТІВ

Єлизавета Богданова, Тетяна Чорна, Сергій Малахов

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
xa12850323@student.karazin.ua, tatyanachernaya2002@gmail.com, malakhov@ karazin.ua

Надійшла: жовтень 2022. Прийнята: листопад 2022.

***Анотація:*** *Розглянуто проблематику експлуатації вразливостей програмного забезпечення. Звернено увагу на існування двох іпостасей практичного застосування експлойтів: - як інструменту атаки та, як засобу тестування інформаційних систем, що потребують захисту. Підкреслено, що частіше всього експлойти поділяють за типом вразливості безпеки, що експлуатується. Аналіз відомих інцидентів, пов'язаних з використанням експлойтів, дозволяє стверджувати про існування зв'язку між ступенем популярності програмного продукту або пристрою та ймовірністю створення відповідних експлойтів. Звернено увагу на те, що N–day експлойти складають суттєву частину існуючих загроз безпеки для вразливих пристроїв (систем). Головною причиною подібного становища є, несвоєчасне оновлення використовуваного програмного забезпечення та ігнорування оновлень патчів безпеки. Підкреслено надзвичайну важливість своєчасного випуску патчів безпеки, як ефективного засобу парірування виявлених уразливостей програмного забезпечення. Звернено увагу на те, що процес випуску патчів безпеки є базовою складовою у спектрі можливих захисних реакцій, при вирішенні подібних проблем. Зроблено акцент на тому, що за результатами аналізу відомих випадків протиправного використання експлойтів (за останні 3 роки) вони, в своєї переважній більшості, спрямовані на 3-х векторах атак: - відмова в обслуговуванні; - неправомірне розширення (підвищення) існуючих повноважень управління; - віддалене виконання зловмисного коду.*

***Ключові слова****: експлойт; програмна вразливість; патч безпеки; інформаційна безпека.*

## 1. Вступ

Відомо, що вразливості можуть бути присутні в будь-якій складовій сучасних інформаційних систем: - операційна система (ОС), програмне забезпечення (ПЗ), апаратне забезпечення, Web-сервісі [1]. В будь-якому випадку потенційні кібер зловмисники будуть постійно намагатися сканувати програмно апаратні ресурси обраної жертви та вести мережеву розвідку щодо параметрів використовуваних Web-сервісів [2], щоб знайти вразливість в периметрі безпеки цільової системи, а потім, за допомогою відповідного експлойту забезпечити необхідні умови для подальшої реалізації потрібних несанкціонованих дій [3]. Крім того, самі користувачі (персонал) потенційної жертви атаки, може ненавмисно (несвідомо) сприяти появі додаткових вразливостей інформаційної безпеки (ІБ), наприклад, використовуючи слабкі параметри настроювань конфіденційності у своїх соціальних мережах та/або облікових записах електронної пошти, та/або ставши жертвою інтегрованої багатоходової атаки, з використанням прийомів соціального інжинірингу (*т.з., SE-атак*) [4-5].

Кіберзлочинці можуть використовувати експлойти для різних цілей: від маніпуляцій з окремим локальним атакованим пристроєм до масштабних комп'ютерних злочинів з залученням до атаки заздалегідь скомпрометованих ними мережевих ресурсів, різних за масштабами ІТ структур. Фізично, завдяки експлойтам зловмисники можуть заблокувати доступ до скомпрометованого ними пристрою та/або системі, контролювати роботу використовуваних Web-сервісів та/або процесів, отримати доступ до конфіденційній службовій або персоніфікованій інформації (доксинг) [6], вимагати гроші у жертви та проводити акції з кібербулінгу [4-5]. Однак, поряд з цім, за допомогою програм експлойтів, фахівцями з ІБ можуть завчасно тестуватися на проникнення їх ІТ інфраструктуру, що дозволяє імітувати різні вектори атак на корпоративні ресурси та служби.

Оскільки у пошуку вразливостей зацікавлені обидві сторони, то випущених експлойтів стає все більше. Очевидно, що для упорядкування цього напрямку діяльності, необхідна кла-

 

сифікація, як вже існуючих, так і майбутніх експлойтів, що полегшить запобігати діям потенційних зловмисників і впорядкувати роботу фахівців щодо визначення вразливостей ІБ.

## 2. Основна частина

Станом на сьогоднішній день, існують два основних класи експлойтів, відомих серед профільних фахівців як, *N-day* експлойти та експлойти нульового дня (т.з. *zero-day, зеродеї*).

Атаки нульового дня, як правило, привертають до себе увагу, коли йдеться мова про загрози кібербезпеці, але , нажаль, найчастіше, саме відома вразливість *N-day* є набагато більш серйознішою проблемою для багатьох сучасних організацій. *N-day* експлойт - це вразливість, що вже відома, та для якої вже доступне відповідне виправлення [7]. Тобто після публікації патчу безпеки і CVE (*з англ. Common Vulnerabilities and Exposures*) вразливості, експлойт нульового дня стає *N-day* експлойтом (Рис. 1).

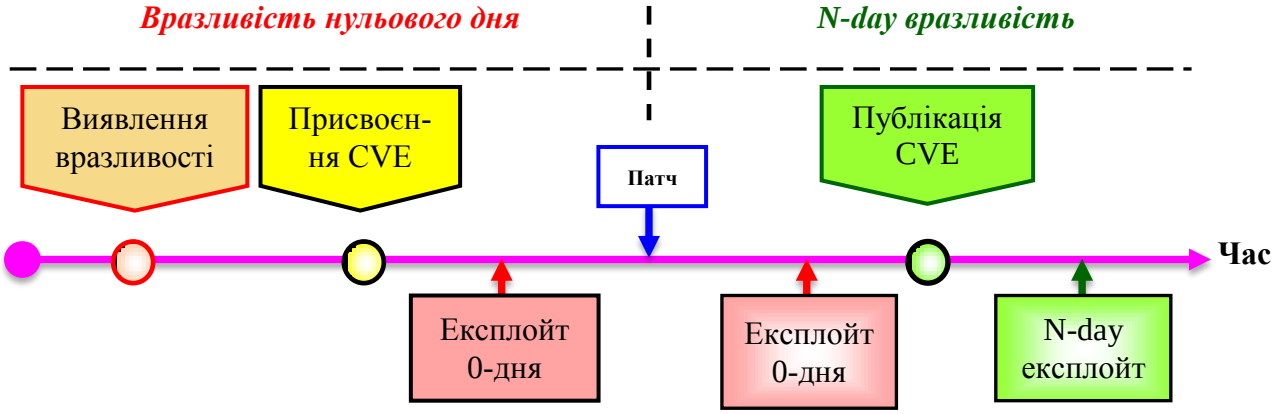


Рис. 1 – Алгоритм реагування на вразливості та публікації експлойтів

Теоретично, «застарілі» експлойти не повинні були б загрожувати безпеці пристроїв та ПЗ, проте вони, нажаль, продовжують використовуватися для атак і продовжують набирати популярності. Певною мірою це зумовлено тим, що зловмисники можуть дізнаватися про подробиці існуючих вразливість все, що їм потрібно, шукаючи відповідні виправлення (т.з. *«бінарне порівняння»)*, або переглядаючи загальнодоступні документи на наявність активних експлойтів. Також є можливість, що постачальники ПЗ та/або телекомунікаційного обладнання, не надають оновлення безпеки для своїх попередніх «продуктів», навіть якщо вони випускають відповідне виправлення ПЗ, або ж самі користувачі не встановлюють своєчасно патчі безпеки. Прикладом може бути відомий *N-day* експлойт *EternalBlue*, який був досить активним (*як інструмент для здійснення атак*), навіть через три роки (з 2017-2020 рр.) після випуску відповідного патчу. Серед іншого, він був використаний програмою-вимагачем *WannaCry*, а за даними *Shodan*, понад 650 000 підключених до Інтернету пристроїв все ще залишаються вразливими для нього[8]. Залежно від способу отримання доступу до вразливого ПЗ, існуючи експлойти умовно поділяються на ***віддалені*** (англ. *remote*), ***локальні*** (англ. *local*) та експлойти ***підставного серверу*** [9].

***Віддалений*** експлойт, використовуючи вразливість без попереднього доступу до вразливої системи (пристрою), дозволяє зловмиснику отримати доступ до неї через мережу [10]. В залежності від того, який сервіс експлуатується, атакуючий отримує права користувача або *root* на сервері, що атакується. Після того, як зловмисник сканує сервер на наявність будь-яких відомих локальних експлойтів, якщо такі знаходяться, він використовує їх для отримання *root*-доступу на сервері. В разі, коли зловмисник отримує *root*-доступ, то він може

встановити руткіти (та/або бекдори) [11], які дозволять йому несанкціоновано увійти в скомпрометовану їм систему, та почати «працювати» на цільовому сервері без загрози його відстеження з боку адміністратора та/або інших користувачів. Найбільш поширеними різновидами *віддалених* експлойтів є переповнення буферу (*використання вразливості CVE-2015-0311, тобто переповнення буфера Adobe Flash Player, яка дозволяє зловмисникам віддалено виконувати довільний код через невідомі вектори атак*)[12] та інші атаки з неперевіреним введенням. Вони виконуються або для загальнодоступних служб (таких, як HTTP та FTP), або під час входу до захищених служб (таких, як POP та IMAP).

***Локальний*** експлойт активується безпосередньо у вразливій системі (пристрої), вимагаючи попереднього доступу до неї, що дозволяє звичайному користувачеві отримати *root*-права, виконавши певну послідовність дій. Як правило, ці експлойти виникають в тому випадку, коли будь-яка привілейована програма містить помилку, яка не виконує достатніх перевірок користувача перед виконанням команди з правами суперкористувача (суперюзера).

Експлойти ***підставного серверу*** - це вразливість по відношенню до існуючих клієнтських додатків, що зазвичай включають змінені сервери, які розсилають експлойти при отриманні доступу до клієнтського додатку. Ця вразливість з «успіхом» працює в парі із SE–атаками, наприклад: фішинг і ланч-фішинг (для розповсюдження рекламного ПЗ) [9].

Очевидно, що без існування вразливостей не буде експлойта, оскільки саме вони і є умовною «точкою входу» для експлойтів в систему (апаратний пристрій), що атакується. Відповідно, логічно класифікувати експлойти за типом уразливості, яку вони використовують, наприклад [13]: - переповнення буферу; міжсайтовий скриптинг; підробка міжсайтових запитів; SQL-ін'єкція; атака повернення до бібліотеки та інші.

Існують загальна система оцінки вразливостей CVSS 2.0 (*Common Vulnerability Scoring System*) та рівень загрози експлойту, за допомогою яких можна дізнатися ступінь небезпеки для пристрою, що атакується. На рис. 2-3 приведені відомості CVSS та рівень загроз експлойту, станом на 2019–2022 р. Як можна помітити 34% відомих експлойтів мають високий рівень загрози (CVSS ≥ 7), а 54% експлойтів мають середній рівень (CVSS < 7 та CVSS ≥ 4). Тобто, 88% загальнодоступних експлойтів розроблені для вразливостей середнього чи високого ступеня небезпеки [13, 14].

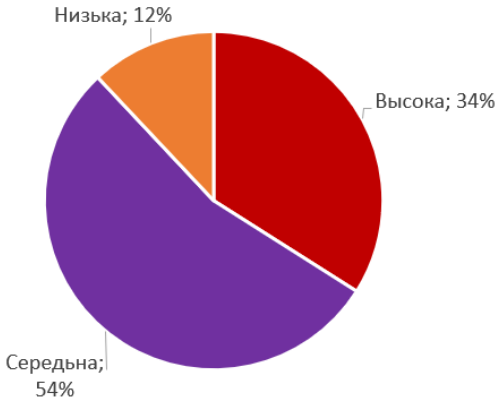


Рис. 2 – Розподіл експлойтів за рівнем загрози вразливості

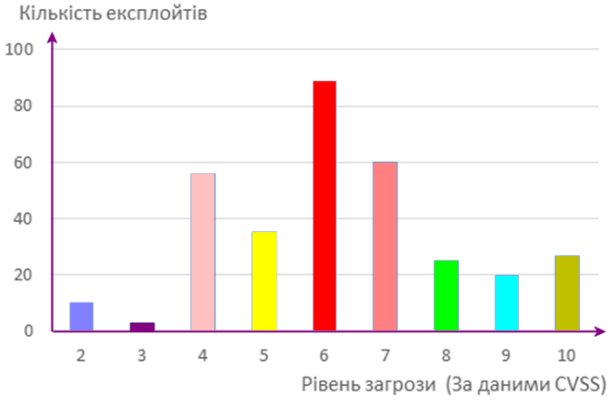


Рис. 3 - Експлойти, що класифіковані за рівнем загрози вразливості CVSS *(2019-2022 рр)*

Відома, також, і інша класифікація експлойтів по здійснюваним діям щодо вразливої цільової системи: - несанкціонований доступ до даних (*наприклад, копіювання, видалення або модифікація*); - віддалене виконання коду (*RCE - Remote Code Execution*); - відмова в обслуговуванні; - підвищення привілеїв користувачів; - обхід (блокування) окремих функції

безпеки; - довільне читання файлів; - пошкодження пам'яті; - несанкціонована зміна налаштувань мережевих засобів (*наприклад, модифікація таблиці комутації адресів роутерів*) та інші [9, 12]. Так наприклад, на рис. 4 наведено діаграми, які демонструють розподіл експлойтів по роках (*за 2019-2022 рр.*), що найчастіше застосовували різні вразливості атакованих систем [12, 15]. Як видно з діаграми найактуальнішими, отже затребуваними, є експлойти для віддаленого виконання коду, відмови в обслуговуванні та підвищення привілеїв.

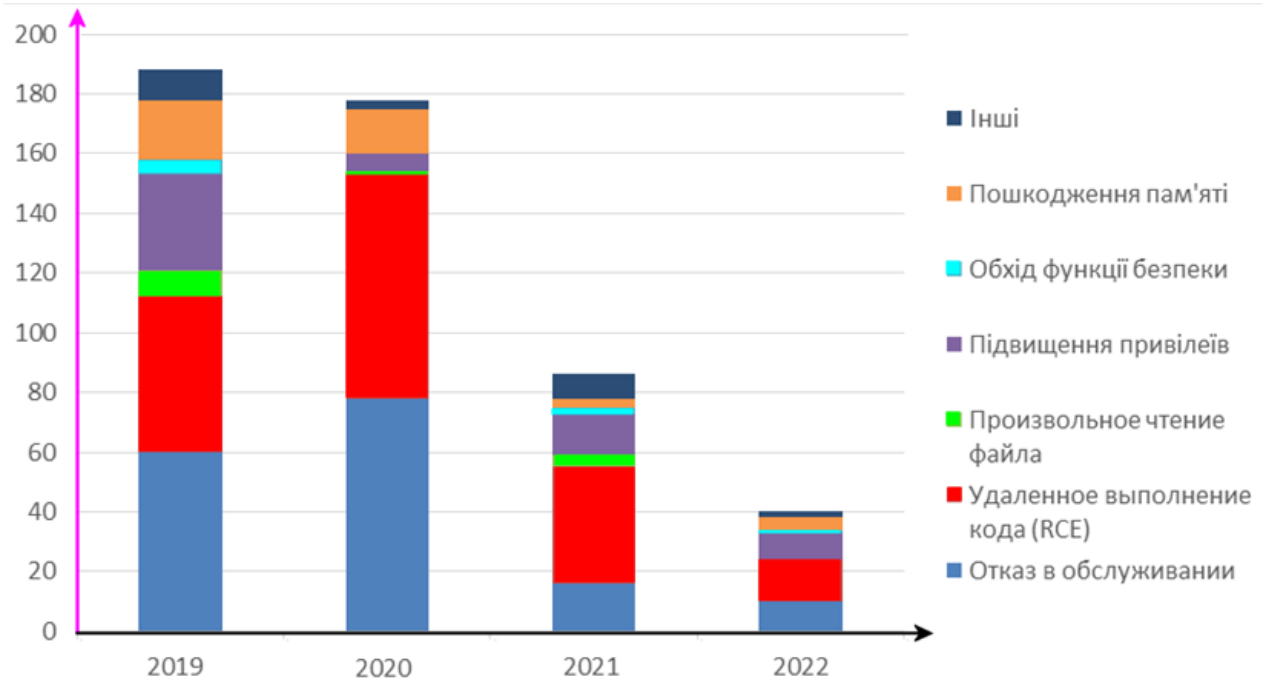


Рис. 4 – Використання та розподіл експлойтів за частотою використання вразливостей, що експлуатується *(за даними CVE)*

Оскільки експлойти мають своєю головною ціллю забезпечення виконання, потрібних для атакуючого, несанкціонованих дій на вразливій системі та/або пристрої, то вони можуть бути класифіковані по кінцевих об'єктах їх застосування [9, 12], наступним чином:

- Експлойти ОС. Вразливості ОС є точками входу для експлойтів, що можуть пошкодити роботу функціоналу пам'яті або призвести до некоректної роботи пристрою.
- Експлойти офісних програм. Вразливості офісного ПЗ найчастіше використовуються зловмисниками для того, щоб в наступному, скомпрометувати всю його систему, та поширити шкідливе ПЗ (*Cobalt Strike*) [16]. Використання каналу проникнення через вразливості офісних програм обумовлено значною поширеністю пакетів офісного ПЗ, практично для всіх типів існуючих платформ (ПК, хмарні додатки, гаджети тощо). При цьому не вчасно виконане оновлення такого ПЗ чи патчів безпеки, створює потрібні передумови для наступної атаки з використанням даної категорії експлойтів.
- Експлойти для спеціального ПЗ.
- Експлойти для Web-серверів, зокрема для найбільш поширених Інтернет браузерів (*Chrome, Firefox тощо*) або Web-сайтів (*facebook.com, livejournal.com*). Такого виду експлойти часто можуть не завдавати шкоди даних, що зберігаються на пристрої.

- Експлойти для апаратних прошивок. «Вдале» використання таких вразливостей виключає необхідність обходити будь-які засоби захисту ОС. При цьому, адаптація відповідного експлойта для різних ОС не складе труднощів, що обумовлено тим, що низькорівневі компоненти ядра для роботи з апаратним забезпеченням на багатьох ОС, практично однакові [17].

## 3. Висновки

Експлойти нульового дня, еволюційно породжують *N-day* експлойти (рис. 1), які складають суттєву частину загроз для вразливих пристроїв, саме через несвоєчасне оновлення ПЗ та/або ігнорування випусків (оновлення) відповідних патчів безпеки.

Віддалені експлойти «працюють» через мережу, використовуючи наявну вразливість у захисті без попереднього доступу до цільової вразливої системи. Локальні експлойти, навпаки, запускаються у вразливому пристрої (системі), однак потребують попереднього доступу до неї. Ці обидва різновиду експлойтів позиціонуються, переважно як засіб для отримання повноважень суперюзера.

Для ефективної експлуатації серверної вразливості, експлойту потрібно сформувати та надіслати на сервер відповідний запит, що містить шкідливий код, проте потрібно якось примусити (переконати) потенційну жертву підключитися до підробленого серверу. В цьому разі ефективним спойлером експлойту є використання одного із різновидів SE–атак.

Частіше всього експлойти поділяють за типом вразливості, що експлуатується при цьому, за сукупністю підтверджених випадків їх застосування, більшість експлойтів, які використовуються зловмисниками для здійснення потрібних їм несанкціонованих дій у вразливих системах, в своєї переважній більшості спрямовані на: - відмову в обслуговуванні, підвищення діючих повноважень (привілеїв) та віддалене виконання зловмисного коду.

## Список літератури


[1] Богданова, Е., & Малахов, С. (2022). Обобщение специфики применения эксплойтов. Збірник наукових праць SCIENTIA, (Vol.2), 28-32. https://ojs.ukrlogos.in.ua/index.php/scientia/issue/view/24.06.2022/759 Available at: DOI 10.36074/scientia-24.06.2022

[2] Кохановська, Т., Нарежний, О., & Дьяченко, О. (2020). Дослідження можливостей технології Honeypot. Комп'ютерні науки та кібербезпека, 1(1), 33-42. https://doi.org/10.26565/2519-2310-2020-1-03

[3] Мелкозьорова, О., Лєсная, Ю., & Малахов, С. (2022). Особливості забезпечення захисту від НСД в сучасних інформаційних системах. InterConf, (97), 506-511. Вилучено із https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/18428

[4] Погоріла, К., Лєсная, Ю., Богданова, Є., & Малахов, С. (2022). Соціальний інжиніринг, як фактор реалізації інсайдерських загроз. InterConf, (111), 494-501. Вилучено із https://interconf.top/documents/2022.06.6-8.pdf

[5] Гайкова, В., & Малахов, С. (2021). Аналіз факторів і умов реалізації кібербулінгу з урахуванням можливостей сучасних інформаційних систем. Комп'ютерні науки та кібербезпека, (1), 50-59. https://doi.org/10.26565/2519-2310-2021-1-04

[6] Чорна Т., Богданова Є., Погоріла К. Проблематика доксингу: - міжнародний досвід щодо забезпечення захисту персональних даних // Study of world opinion regarding the development of science. Proceedings of the IX International Scientific and Practical Conference. Prague, Czech Republic. 2022. Pp. 720-723 URL: https://isg-konf.com/study-of-world-opinion-regarding-the-development-of-science/ Available at: DOI: 10.46299/ISG.2022.2.9

[7] (2021). N-Day Exploit Protection Strategies. Вилучено із: http://surl.li/dsecc

[8] (2022). Предупреждение функции «Анализ сети» Avast: «Уязвимость для атаки WannaCry/DoublePulsar» Вилучено із: http://surl.li/dsecd

[9] (2017). Эксплойты, (Exploits). Вилучено із: http://surl.li/delac

[10] REMOTE SERVICES EXPLOITATION - DEFINITION, EXAMPLES, & PREVENTION – EXTRAHOP. Вилучено із: http://surl.li/dseci

[11] Ализар А. (2013). Каталог эксплойтов АНБ. Хакер, (280). Вилучено із: https://xakep.ru/2013/12/31/61833/

[12] Exploit Database. Вилучено із: http://surl.li/dseck

[13] Common Vulnerability Scoring System version 3.1: Specification Document. Вилучено із: https://www.first.org/cvss/examples

[14] 2022 CWE Top 25 Most Dangerous Software Weaknesses. Вилучено із: http://surl.li/

[15] (2022). Список 25 самых используемых эксплойтов. Вилучено із: http://surl.li/dseco

[16] Никитина Т. (2022). Фейковый PoC устанавливает на машину ИБ-экспертов Cobalt Strike Beacon. Вилучено із: http://surl.li/dsecy

[17] Лянин Чжао, Дэвид Ли. (2021). Аппаратные и программные решения: что опаснее? Вилучено із: https://www.osp.ru/os/2021/01/13055832

Received: October 2022. Accepted: November 2022.

**Authors:**
Yelyzaveta Bohdanova, 4rd year student, Faculty of Computer Science, Kharkiv National University named after V.N. Karazin, Kharkiv, Ukraine.
**E-mail**: xa12850323@student.karazin.ua
Chorna Tetiana, 4rd year student, Faculty of Computer Science, Kharkiv National University named after V.N. Karazina, Kharkiv, Ukraine.
**E-mail**: tatyanachernaya2002@gmail.com
Serhii Malakhov, Ph.D., Senior Researcher, Computer Science Department, V.N. Karazin Kharkiv National University, Ukraine.
**ORCID ID** https://orcid.org/0000-0001-8826-1616
**E-mail**: malakhov@karazin.ua

**Overview of the current state of threats caused by the influence of exploits.**

**Annotation.** The issue of exploiting the software vulnerabilities is considered in the article. Particular attention has been paid to the two aspects of the practical usage of exploits, as an attack tool and as a means of testing protected information systems. It is emphasized that most often exploits are divided by the type of security vulnerability exploited. Analysis of the known incidents related to the use of exploits, al-lows us to assert the existence of a relationship between the degree of popularity of a software product or device, and the probability of the exploits being created. Attention is drawn to the fact that N-day exploits constitute a significant part of existing security threats for vulnerable devices (systems). The main reason for this situation is untimely updating of the used software and ignoring updates of security patches. The extreme importance of the timely release of security patches as an effective means of preventing the usage of identified software vulnerabilities is emphasized. Releasing security patches is a basic element of possible defensive reactions when dealing with such issues. Attention is drawn to the fact that, according to the results of the analysis of known cases of illegal use of exploits (the last 3 years), they, in their vast majority, are aimed at 3 attack vectors: - denial of service; - illegitimate widening the current powers of managemention; - remote execution of malicious code.

**Keywords:** exploits; software vulnerabilities; security patches; information security.