УДК 004.738.5(043.2)

О.В. Дубчак,
О.О. Левченко,
І.А. Кравчук
Національний авіаційний університет, Київ

АНАЛІЗ УРАЗЛИВОСТЕЙ ВЕББРАУЗЕРА

У 2022 р., за даними Державного центру кіберзахисту, зареєстровано перевишення кількості кіберінцидентів майже у три рази відносно 2021 р. Питання безпеки користувачів мережі Інтернет, що напряму залежить від програмного забезпечення, використовуваного для доступу до вебсайтів та їхнього перегляду – веббраузерів (ВБ), залишається пріоритетним, оскільки саме кількість подій інформаційної безпеки в категоріях «Шкідливий програмний код» та «Збір інформації зловмисником» зросла у 18,3 та 2,2 рази відповідн [1].

Як відомо [2], ВБ є своєрідними «воротами», що надають доступ до мережі Інтернет, отже безпека ВБ є важливим критерієм захисту даних користувача від несанкціонованого доступу.

Станом на березень 2023 р., за даними StatCounter, найпоширенішим у світі ВБ є Google Chrome (64,8%), на другому місці Apple Safari (19,5%), далі - Edge (4,63%), Mozilla Firefox (2,93%), Samsung Internet (2, 57%) та Opera (2.33%). В Україні найпопулярнішим стабільно залишається Google Chrome (понад 66%), далі - Opera (12,97%), Safari (9,41%), Firefox — 4,48% та Samsung Internet — 1,78% [3].

Майже третина всіх ВБ містить критичні вразливості: Microsoft Internet Explorer і Edge – понад 40%;Google Chrome – майже 40%; Mozilla Firefox – 35%; Opera – 34%; Safari - майже 30%, відповідно до звіту дослідників Інтернет-безпеки щодо стану сучасних ВБ [4].

Причому, серед вразливостей ВБ найбільший відсоток припадає на ті, що спрямовані на отримання даних.

Користувачу важливо розуміти функціональність та можливості використовуваного ВБ - увімкнення за вмовчання деяких функцій ВБ може не тільки полегшити роботу, але й знизити рівень безпеки.

Серед конкретних особлививостей ВБ та пов'язаних з ними ризиків наявні наступні вразливості: ActiveX – технологія, що використовується Microsoft Internet Explorer у системах Microsoft

Windows; вразливості Java - успішні атаки вразливості можуть призвести до несанкціонованого доступу для читання даних, доступних для Java SE; вразливості JavaScript/VBScript – зловмисники можуть додавати значну кількість функцій та інтерактивності до вебсторінки; вебвідстеження – використовується для запам'ятовування і розпізнавання відвідувачів вебсайту.

Слід зауважити, що техніка вебвідстеження (ВВ) достатньо швидко розвивається останнім часом: І-е покоління приймає встановлені сервером ідентифікатори (файли cookie та evercookie); ІІ-ге покоління - відбиток браузера, ідентифікує пристрій на основі його унікальних конфігурацій (часовий пояс, системні шрифти, модулі до ВБ та їхні версії, журнал відвідувань, розширення екрану).

З одного боку, за допомогою ВВ можлива автентифікація користувачів, з іншого - ВВ може використовуватися для надання персоналізованих послуг. Причому, за умови, що надана послуга є небажаною, наприклад, небажана цільова реклама, таке ВВ становитиме порушення конфіденційності [5].

Отже, технологія ВВ багато в чому небезпечніше інших уразливостей ВБ, оскільки є підґрунтям загрози порушення конфіденційності даних користувача. Слід також зазначити, що захист від ВВ може бути проблематичним, оскільки неможливо дізнатися щодо наявності відслідковування дій користувача.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Звіт Державного центру кіберзахисту. [Електронний ресурс] - Режим доступу: https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit

2. What is a web browser? [Електронний ресурс]– Режим доступу: https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/

3. Статистичний звіт StatCounter [Електронний ресурс] - Режим доступу: https://gs.statcounter.com/browser-market-share/desktop-tablet-console/worldwide

4. Internet browser vulnerability and user security [Електронний ресурс] - Режим доступу:https://augustafreepress.com/news/internet-browser-vulnerability-and-user-security/

Yinzhi Cao. (Cross-)Browser Fingerprinting via OS and Hardware Level Features [Електронний ресурс]– Режим доступу: http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf