Секція 1

ПЕРЕПОВНЕННЯ БУФЕРА

Корінчук В.І.
Національний аерокосмічний університет ім. М.Є Жуковського
«Харківський авіаційний інститут»
Науковий керівник Пєвнєв В.Я

Актуальність. Переповнення буфера був і залишається дуже важливою проблемою в аспекті безпеки програмного забезпечення. Саме з можливістю використання нападів на переповнення буфера для видалення шкідливого коду, який пов'язаний з постійними дискусіями, та галасуванням навколо нападів цього класу. Проблема переповнення буфера протягом багатьох років лише стала складнішою, з'явилися інші типи атак, і, як наслідок, були розроблені принципово нові напади на переповнення буфера.

Мета. Запобігти переповнення буфери, ознайомитися з причинами переповнення та їх уникнення

Основні положення. Переповнення буфера – це, мабуть, одна з найцікавіших і найпоширеніших вразливостей програмного забезпечення. Це може призвести до пошкодження даних, збоїв у програмі та навіть до шкідливого коду. Здається, це невелика помилка програміста (за особливих обставин), щоб дозволити розлюченому хакеру зробити майже все на комп'ютері невинного користувача програми [2].

Помилка полягає в тому, що в будь-якому місці програми дані копіюють з одного розділу пам'яті в інший, не перевіряючи, чи є для них достатньо місця, де вони копіюються. Область пам'яті, де дані копіюються, зазвичай називають буфером. Таким чином, якщо є занадто багато даних, то частина їх виходить за межі буфера – існує «переповнення буфера» [1]. Відомі такі типи атак, які здійснюються за рахунок переповнення буфера: напади на стек, напади на формат лінії та напади на хіп.

Цікавим фактом є те, що переповнення буфера є однією з найпоширеніших причин, чому атака можливі за допомогою довільного коду через вразливості [3]. Крім того, багато програм, розроблених класичними мовами, такими як C та C ++, вважаються дуже чутливими до цього типу проблем.

Серед найефективніших заходів протидії цим типам нападів необхідно розрізнити наступні: своєчасна перевірка даних, введення «точок попередження» та використання сучасних мережевих екранів.

Висновок. Наприкінці розгляду основних методів боротьби з атаками переповнення буфера слід зазначити, що, звичайно, компетентне програмування залишається найбільш ефективним і в той же час найважче

реалізованим способом. Саме якісно складений код зможе найбільш ефективно витримати всілякі спроби зовнішніх злому.

Список літератури

1. Захист від переповнення буфера. *Wiki*. URL: https://uk.zahn-info-portal.de/wiki/Buffer_overflow_protection (дата звернення: 20.11.2022);
2. Способи реалізації атак переповнення буфера. *Blocklist.net*. URL: http://um.co.ua/10/10-6/10-6472.html (дата звернення: 20.11.2022);
3. Фэрроу, Р. Атаки на сеть через переполнение буфера: технологии и способы борьбы // Защита информации. INSIDE. – 2006. – № 4.

Відомості про авторів

Корінчук Валентина Ігорівна, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 095-691-07-75, Valyakorinchuk@gmail.com
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu