Автор:
Джалі Назар Самірович,
студент 21 ІПЗ групи
Науковий керівник:
Малежик Петро Михайлович,
кандидат фізико-математиних наук,
старший викладач кафедри
комп'ютерної інженерії та освітніх
вимірювань

ПРОБЛЕМА РЕАЛІЗАЦІЇ ЗАХИСТУ ВІД ВРАЗЛИВІСТІ MELTDOWN CVE-2017-5754 В СУЧАСНИХ ПРОЦЕСОРАХ

Анотація. Метою дослідження є аналіз проблеми реалізації захисту від вразливостей сучасних процесорів. Завданням дослідження є порівняння та вибір підходів реалізації захисту від вразливості meltdown cve-2017-5754 сучасних процесорів.

Ключові слова: процесор, вразливість, спекулятивне виконання команд.

Вступ. 3 січня 2018 року спільноті була офіційно оприлюднена вразливість meltdown одночасно з атакою spectre. Вразливість стосувалася процесорів виробництва Intel, що випущені у період з 1995 року (крім Intel Itanium та Intel Atom після 2013 року) по 2018 рік, а також ARM процесорів з ядром cortex-A75.

Постановка задачі. З допомогою meltdown можливо зчитувати всю пам'ять, до якої навіть відсутній доступ. Вразливість зачепила широке коло систем, починаючи з мобільних смартфонів, вбудованих систем і закінчуючи хмарними сервісами.

Метою дослідження є аналіз проблеми реалізації захисту від вразливостей сучасних процесорів та існуючих підходів реалізації захисту від їх впливу.

Основна частина. Meltdown використовує таке поняття як стан перегонів (конкуренції), який притаманний багатьом сучасним процесорам. Експлойт виникає в момент часу між доступом до пам'яті та перевіркою доступу під час виконання інструкцій процесора. Вразливість дає можливість злоумислому процесу зчитувати дані з будь-якої ділянки пам'яті, яка призначена поточному простору пам'яті процесора.

Врахочуючи, что конвеєр іструкцій розташований у вражених процесорах, дані, які не повинні бути доступними, будуть з великою ймовірністю завантажені в кеш процесора під час спекулятивного випконання команд, звідти потім і можуть бути відновлені та використані кіберзлочинцем.

Оскільки більшість операційних систем розмічають фізичну пам'ять, процеси ядра та інші процеси користувачів у адресний простір кожного процесу, meltdown робить можливим для злоумисного процесу читати будь-яку фізичну пам'ять, пам'ять ядра та размічену пам'ять інших процесів, незважаючи на те, чи є у цього процесу на це відповідні права. У якості захисту може бути використане уникнення розмітки пам'яті таким вразливим способом (програмне рішення) або модифікація процесора. Атака meltdown не може бути виявлена під час виконання.

За словами генерального директора Брайана Кржанича у середині березня, компанія вже випустила виправлення для всіх продуктів, випущених за останні 5 років (6,7 і 8-е покоління процесорів сімейства Intel Core). Але слід зазначити, що перші виправлення випущені в середині січня призводили на багатьох комп'ютерах до збоїв в роботі, перезавантаженням і BSOD. Хоча з поточними патчами таких проблем не спостерігається, хоча і є певні наслідки.

Наприклад, якщо розглядати спосіб рішення KPTI, при якому пропонувалося вимкнення відображення сторінок пам'яті ядра у адресний простір процесу, то це призводило до втрат продуктивності від 5% до 30%. Зниження продуктивності залежить від того, наскільки часто додаток має справу з ядром операційної системи, чи багато переключень контексту даного процесу або інших його активностей.

Відомі браузери також випустили оновлення, що ускладнюють роботу вразливості meltdown, не даючи злоумисному коду точно виміряти час доступу до пам’яті, зменшуючи точність функцій визначення часу виклику.

Висновки. Незважаючи на наявність вирішення проблеми захисту від вразливості meltdown cve-2017-5754 у сучасних процессорах, мають місце катастрофічні наслідки роботи виправлень для поточних систем, а питання чи варто хвилюватися користувачам комп’ютерів, що використовують процесори, що підпадають під дію вище зазначених вразливостей, залишається відкритим.

Список використаних джерел:

1. ARM Processor Security Update [Електронний ресурс]. Режим доступу до ресурсу: https://developer.arm.com/support/security-update
2. Meltdown [Електронний ресурс]. Режим доступу до ресурсу: https://meltdownattack.com/meltdown.pdf
3. «Без Meltdown и Spectre»: Intel перепроектирует свои процессоры [Електронний ресурс].Режим доступу до ресурсу: https://habrahabr.ru/company/1cloud/blog/352244/
4. Meltdown and Spectre Patching Has Been a Total Train Wreck [Електронний ресурс] https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/
5. Initial Benchmarks Of The Performance Impact Resulting From Linux's x86 Security Changes [Електронний ресурс]. Режим доступу до ресурсу: https://www.phoronix.com/scan.php?page=article&item=linux-415-x86pti