Неужели лишь изменение аппаратного дизайна поможет решить проблему?

Исследователи из Samsung, Сеульского национального университета и Технологического института Джорджии представили новую атаку «TIKTAG», нацеленную на технологию Memory Tagging Extension (Memory Tagging Extension (MTE) – это расширение архитектуры ARM для улучшения безопасности памяти. Оно добавляет теги к блокам памяти и указателям, что позволяет выявлять ошибки, такие как использование освобожденной памяти и выход за границы. При доступе к памяти проверяется соответствие тегов указателя и памяти, что помогает разработчикам обнаруживать ошибки на этапе разработки. MTE минимально влияет на производительность и является частью ARMv8.5-A архитектуры, доступной в современных процессорах ARM." data-html="true" data-original-title="MTE" >MTE) в архитектуре ARM (Advanced RISC Machines) – это архитектура процессоров, разработанная британской компанией ARM Holdings. Она отличается от традиционной архитектуры x86, используемой в большинстве настольных компьютеров и серверов. Процессоры на основе архитектуры ARM обычно используются в мобильных устройствах, таких как смартфоны, планшеты и ноутбуки, а также во многих других встроенных системах, включая микроконтроллеры и смарт-устройства.

 Основным преимуществом архитектуры ARM является ее энергоэффективность. Процессоры ARM потребляют меньше энергии и генерируют меньше тепла по сравнению с процессорами x86, что делает их идеальным выбором для портативных устройств с ограниченными батареями. ARM-процессоры также обладают высокой производительностью и хорошей масштабируемостью, позволяя создавать мощные мобильные устройства.

 ARM Holdings не производит собственные процессоры, а лицензирует свою технологию и дизайн процессоров другим компаниям. Это позволяет партнерам ARM создавать свои собственные процессоры на основе данной архитектуры, адаптированные под различные потребности и рынки." data-html="true" data-original-title="ARM" >ARM. Атака позволяет обойти защитный механизм с вероятностью успеха более 95%.

Memory Tagging Extension (MTE) была введена в ARM v8.5-A для предотвращения повреждений памяти. Она использует 4-битные теги для 16-байтных блоков памяти, чтобы защитить от атак на целостность памяти, проверяя соответствие тегов указателей и памяти.

Исследователи обнаружили, что используя всего два инструмента, TIKTAG-v1 и TIKTAG-v2, можно через спекулятивное исполнение добиться утечки тегов памяти MTE с высокой вероятностью успеха.

Хотя утечка тегов напрямую не раскрывает конфиденциальные данные, такие как пароли или ключи шифрования, она позволяет злоумышленникам подорвать защиту MTE, делая систему уязвимой для атак на повреждение памяти.

TIKTAG-v1 использует спекулятивное сжатие в предсказании ветвлений и предвыборке данных процессора. Этот инструмент эффективен против ядра Linux — это свободная и открытая операционная система, разработанная Линусом Торвальдсом в 1991 году. С тех пор Linux стал одной из наиболее популярных альтернатив коммерческим операционным системам.

 Основное преимущество Linux заключается в его открытом исходном коде, что позволяет пользователям свободно изменять и распространять систему в соответствии с лицензией GNU GPL.

 Linux предоставляет стабильную, надежную и гибкую платформу для работы с компьютером или сервером. Большинство дистрибутивов Linux (например, Ubuntu, Fedora, Debian) поставляются с разнообразными программами и инструментами для работы, включая офисные приложения, интернет-браузеры, мультимедийные инструменты и многое другое.

 Linux также широко используется в серверной сфере и встроенных системах, таких как маршрутизаторы и мобильные устройства." data-html="true" data-original-title="Linux" >Linux, особенно в функциях, связанных со спекулятивным доступом к памяти. Атака требует манипуляции указателями ядра и измерения состояния кэша для определения тегов памяти.

TIKTAG-v2 использует механизм перенаправления данных в спекулятивном исполнении, когда значение сохраняется по адресу памяти и немедленно загружается с этого же адреса. Соответствие тегов позволяет успешно загрузить значение и изменить состояние кэша, в противном случае, перенаправление блокируется и состояние кэша остаётся неизменным. Таким образом, состояние кэша после спекулятивного исполнения позволяет определить результат проверки тегов.

Исследователи продемонстрировали эффективность TIKTAG-v2 против браузера Google Google Chrome – браузер, который разрабатывается на основе свободного проекта Chromium. Для отображения web-страниц браузер использует движок WebKit.

 Первая публичная бета-версия Google Chrome была представлена 2 сентября 2008 года, а первая стабильная версия – 11 декабря 2011 года. Изначально Chrome выпускался только под Microsoft Windows. Позже браузер был выпущен для Linux, macOS и мобильных платформ.

 Браузер Chrome нацелен на повышения уровня безопасности пользователей за счет максимально высокой скорости работы, а также минимально допустимого функционала. Все дополнительные функции в браузер внедряются за счёт сторонних расширений." data-html="true" data-original-title="Chrome" >Chrome, особенно его движка V8 JavaScript, что открывает путь для

эксплуатации уязвимостей повреждения памяти в процессе рендеринга.

Научная работа, опубликованная на arxiv.org, предлагает следующие меры по защите от атак TIKTAG:

ARM признала серьёзность проблемы, однако опубликовала бюллетень, где указала, что утечка тегов не считается компрометацией архитектуры, так как теги не предназначены для хранения секретных данных.

Команда безопасности Chrome также признала проблему, но решила не исправлять её, так как песочница V8 не предназначена для обеспечения конфиденциальности данных памяти и тегов MTE. Более того, браузер Chrome в настоящее время не включает защиту на основе MTE по умолчанию, что делает её менее приоритетной для немедленных исправлений.

Тем не менее, сообщения о проблемах с MTE на устройствах Pixel 8 были переданы команде безопасности Android в апреле 2024 года и были признаны аппаратным дефектом.