Авторы:

Воробьев Данил Сергеевич

студент

Койков Данил Сергеевич

студент

ФГБОУ ВО «Омский государственный технический университет»

г. Омск, Омская область

УЯЗВИМОСТЬ FORESHADOW МИКРОПРОЦЕССОРОВ ПРОИЗВОДИТЕЛЕЙ INTEL

Аннотация*: в данной статье представлена хронология уязвимостей Meltdown и Spectre, описаны их особенности и меры устранения.*

Ключевые слова*: микропроцессор, информационная безопасность, Foreshadow.*

После обнаружения уязвимостей Spectre и Meltdown, была обнаружена еще одна уязвимость в процессорах Intel, которая оказалась более сильной. Две разные группы исследователей обнаружили уязвимость под названием «Foreshadow» и сообщили об этом Intel [1].

Данные уязвимости запускают спекулятивные атаки по стороннему каналу, особенно ориентированные на процессоры Intel. Эксплуатация данных уязвимостей злоумышленником может позволить ему украсть данные, хранящиеся на компьютере жертвы, а также сторонние облачные системы.

Давайте рассмотрим эту новую уязвимость по побочному каналу.

В январе этого года две разные группы исследователей обнаружили уязвимость бокового канала в процессорах Intel. Обе команды, работающие независимо, сообщили об этом Intel, после чего Intel начала дальнейшие расследования. Данная уязвимость была названа «Foreshadow». Foreshadow похож на Spectre и Meltdown по своей природе, тем не менее, наибольшую трудность все же представлял обход мер безопасности, применяемых против Meltdown и Spectre [1].

Ключевой особенностью Foreshadow является его способность нацеливаться на расширение программного обеспечения защиты расширений Intel. «Software Guard Extensions (SGX)» – компонент, ранее невосприимчивый к недостаткам Spectre и Meltdown. SGX – это выделенный компонент в новейших процессорах Intel, который хранит и защищает данные пользователей даже в опасных ситуациях атаки. Ранее обнаруженные уязвимости побочного канала, Spectre и Meltdown не могли нацелиться на данный компонент.

Исследуя механизм взлома Foreshadow, было выяснено, что злоумышленник может использовать эту уязвимость, чтобы прочитать содержимое, хранящееся в SGX. Злоумышленник также может извлечь секретный ключ аттестации устройства.

Уязвимости был дан индекс (CVE-2018–3615) и она была идентифицирована Intel как L1 Terminal Fault(L1TF): SGX. Он достиг базового балла 7.9, что делает его категорированным под «высоким» уровнем опасности. Корпорация Intel дала следующее описание этого недостатка [2].

«Системы с микропроцессорами, использующими спекулятивное исполнение и защитные расширения для программного обеспечения Intel (Intel SGX), могут допускать несанкционированное раскрытие информации, находящейся в кэше данных L1, от пользователя до злоумышленника с локальным доступом пользователя через анализ побочных каналов».

Получив отчеты о Foreshadow, Intel начала с расследований относительно недостатков спекулятивного исполнения побочных каналов. Интересно, что они обнаружили еще две взаимосвязанных уязвимостей, которые одинаково надежны, но имеют несколько разные цели. Вместе эти три уязвимости были помечены как L1 Terminal Fault (L1TF). В дальнейших исследованиях Intel обнаружила еще два связанных недостатка, которые исследователи назвали «Foreshadow-Next Generation».

Обе эти уязвимости также относятся к категории «Высокий уровень», каждый из которых получает базовую оценку 7.1. Среди них первый вариант L1TF (CVE-2018–3620), обозначенный как «L1 Terminal Fault: OS / SMM» от Intel,

включает в себя использование ошибки страницы терминала для доступа к сохраненным данным. Как описано Intel, «Системы с микропроцессорами, использующие спекулятивное выполнение и переводы адресов, могут допускать несанкционированное раскрытие информации, находящейся в кэше данных L1, злоумышленнику с локальным доступом пользователя через ошибку страницы терминала и анализ побочных каналов» [2].

Атаке Foreshadow / L1-terminal-fault были присвоены следующие номера CVE:

– CVE-2018–3615 для атаки на SGX;

– CVE-2018–3620 для атаки на ядро ОС и режим SMM;

– CVE-2018–3646 для атаки на виртуальные машины [2].

С другой стороны, второй вариант L1TF, L1 Terminal Fault: VMM (CVE-2018–3646), дает злоумышленнику привилегии гостевого пользователя для атаки на виртуальную машину. Intel объясняет это следующим образом: «Системы с микропроцессорами, использующие спекулятивные исполнения и переводы адресов, могут допускать несанкционированное раскрытие информации, находящейся в кэше данных L1, злоумышленнику с локальным доступом пользователя с привилегиями гостевой ОС через ошибку страницы терминала и анализ побочных каналов».

Суммируя оба варианта, эти уязвимости нацелены на другие компоненты системы, кроме CPU-SGX. Эти уязвимости направлены на чтение данных, хранящихся в кэше данных L1. Эти данные включают информацию о памяти режима управления системой (SMM), системном ядре памяти (ОС), гипервизорах (VMM) и виртуальных машинах. Foreshadow-NG может оказаться еще более опасным, поскольку он может использовать виртуальную машину, запущенную в стороннем облаке, чтобы обладать всей облачной инфраструктурой. Это связано с тем, что он размывает границы между виртуальными машинами в облачной системе и обращается к данным, хранящимся в виртуальных машинах. Такие уязвимости представляют угрозу для гигантских облачных систем, таких как Amazon AWS и Microsoft Azure [3].

Список литературы

1. В процессоре Intel обнаружены новые ошибки [Электронный ресурс]. – Режим доступа: https://xakep.ru/2018/08/15/foreshadow/ (дата обращения: 26.11.2018).

2. Foreshadow – Intel CPUs Affected By L1TF Vulnerabilities [Электронный ресурс]. – Режим доступа: https://www.swascan.com/foreshadow-intel-vulnerabilities/ (дата обращения: 26.11.2018).

3. Spectre и Meltdown больше не самые опасные атаки на CPU Intel [Электронный ресурс]. – Режим доступа: https://habr.com/company/crossover/blog/420291/ (дата обращения: 26.11.2018).