Гужанков Евгений Геннадьевич
студент
Воробьев Данил Сергеевич
студент
Уваровский Владислав Вадимович
студент
ФГБОУ ВО «Омский государственный
технический университет»
г. Омск, Омская область

УЯЗВИМОСТИ MELTDOWN И SPECTRE МИКРОПРОЦЕССОРОВ ПРОИЗВОДИТЕЛЕЙ AMD, ARM И INTEL

Аннотация*: в данной статье представлена хронология уязвимостей Meltdown и Spectre, описаны их особенности и меры устранения. По мнению авторов, на данный момент проблема уязвимостей всё ещё является актуальной и, так как не все производители предают ей большое значение, необходимо искать другие компромиссные решения.*

Ключевые слова*: микропроцессор, информационная безопасность, Spectre, Meltdown.*

Ещё в июне 2017 года исследователи команд Грацкого технического университета сообщили фирмам Intel, AMD и ARM о найденных уязвимостях Meltdown и Spectre в архитектуре их микропроцессоров. В большинстве из них заложен принцип внеочередного исполнения команд [1].

Но командами-исследователями было принято решение о не обнародовании столь критических уязвимостей при условии, что фирмы-производители исправят эту проблему в течение полугода. Также они предложили два варианта решения этой проблемы: KAISER (Kernel Address Isolation to have Side-Channels Efficenty Removed, то есть «изоляция адресов ядра для устранения побочных каналов») и KASLR (Kernel Access Layout Randomization или «Рандомизация путей доступа к ядру»).

Особенность данных уязвимостей в том, что их причина кроется не в программном обеспечении, как чаще всего бывает, а в самой архитектуре микропроцессоров, построенной на алгоритме внеочередного исполнения команд. И это позволяет злоумышленникам, путём некоторых манипуляций, получить доступ к личным данным пользователей.

Исследователи объединили уязвимости в 2 группы и назвали их Meltdown (расплавление) и Spectre (призрак), соответственно. Тестирование было произведено на системах Mac OS X, Windows 10, а также на Linux.

Так, Meltdown как бы разрушает изоляцию между операционной системой и пользовательскими приложениями при спекулятивном выполнении команд (т.е. просчёте процессором заранее сценария выполнения команд, необходимых для работы программы). Он игнорирует все защитные меры изоляции адресного пространства так же легко, как и среду паравиртуализации и, в связи с этим, любой защитный механизм построен без учёта этого положения.

При воздействии на системы, Meltdown препятствует обращению к памяти других процессов или пользователей в облаке, независимо от их прав доступа и привилегий, так или иначе затрагивая миллионы пользователей по всему свету. И это делает возможным доступ вредоносной программы к оперативной памяти ядра и считыванию из неё закрытых данных.

Данной уязвимости подвержены многие из процессоров процессоры, выпущенных компанией Intel с 1995 года, за исключением Intel Itanium и Intel Atom.

Уязвимость под названием Spectre («Призрак»), подразумевающее под собой, на самом деле, целых 2 уязвимости, делает возможным вредоносной программе считывать данные, например, пароли, введённые в интернет-браузере. Этой же уязвимости подвержены не только процессоры Intel, но также ARM и AMD.

То есть, были обнаружены уязвимости практически всех электронных устройств, начиная со смартфонов и заканчивая персональными компьютерами. Не маловажной особенностью этих уязвимостей так же является их

незаметность: практически невозможно отследить такой способов кражи данных и получения несанкционированного доступа к ним.

3 января 2018 года Intel заявила о невозможности повреждения данных благодаря этим уязвимостям. Однако открытым остался вопрос их кражи.

Компания Apple подтвердила уязвимость всех процессоров, встроенных в продукцию. Google заявили, что успешно справились с этими проблемами – и опубликовали свои технические решения по борьбе с ними.

Использовать Spectre гораздо сложнее, но тоже возможно. Одним из первых был обновлен браузер Firefox.

В январе 2018 года Apple и Microsoft выпустили обновления для устранения Meltdown на своих операционных системах. 8 января к ним присоединились Intel.Однако, всё выпущенные обновления приводили к замедлению работы систем в среднем на 30%. В том же месяце компания AMD заявила о невосприимчивости своих продуктов к уязвимости Meltdown, но не к Spectre, и поэтому порекомендовала устанавливать обновления, выпускаемые поставщиками программного обеспечения. Однако, частые жалобы обладателей AMD на частые зависания вынудили Microsoft приостановить раздачу обновлений на эти процессоры.

Уже 22 января 2018 года Intel официально попросила пользователей воздержаться от установки последних обновлений, выпущенных компанией. Причиной этого стали жалобы пользователей на частые перезагрузки компьютеров.

15 марта 2018 года Intel рассказала о разрабатываемых моделях процессоров линеек Xeon Scalab и Core восьмого поколения. По словам разработчиков, они будут лишены означенных выше уязвимостей. В частности, этого хотят добиться внедрением новой системы сегментирования.

Также Intel дала понять, что в начале марта 2018 года были выпущены обновления для всех моделей процессоров, выпущенных с 2013 года, а также для ядер Intel Core второго поколения (Sandy Bridge) и более новых процессоров, включая линейки Xeon и HEDT. В дальнейшем они планируют обновить программное обеспечение процессоров серии Core первого поколения, а серии Core 2, построенных на 45-нм технологии. Процессоры 65-нм поколения Core 2

(Conroe и т. д.) планируется обновлять. Иначе говоря, Intel планирует обновить большую часть процессоров, выпущенных с 2007 года [3].

На данный момент проблема уязвимостей всё ещё актуальна и, так как не все производители предают ей большое значение, а имеющиеся решения идут в ущерб производительности, а, в некоторых случаях, вообще к потере работоспособности, необходимо искать другие компромиссные решения.

Список литературы

1. Горбачев А. Найденные в процессорах уязвимости касаются почти всех современных компьютеров и телефонов. Как с ними бороться? / Горбачев А., Филимонов А. [Электронный ресурс]. – Режим доступа: https://meduza.io (дата обращения: 14.02.18)

2. Intel исправила аппаратные уязвимости Meltdown и Spectre [Электронный ресурс]. – Режим доступа: https://tproger.ru (дата обращения: 21.03.2018)

3. В процессорах Intel найдена критическая уязвимость, а патч к ней замедляет работу системы [Электронный ресурс]. – Режим доступа: https://tproger.ru (дата обращения: 21.03.2018)