Автор: Алина Саратова НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 3700 07.01.2018, 13:58
14

Чипокалипсис Intel: что это такое и кому надо бояться

Новый год принес новый скандал. Зародился этот скандал еще в середине 2017 года, но компании, причастные к ЧП, всеми силами старались скрыть его от глаз и ушей общественности. Не вышло. Информация выплеснулась на страницы печатных изданий, в интернет и на ТВ, и теперь практически весь мир гадает: а чем все закончится? Мы решили не оставаться в стороне, и тоже собрали максимально подробную информацию о ситуации, окрещенной в западной прессе Чипокалипсисом. Итак: что происходит, кому надо бояться и чем дело кончится.

Ты помнишь, как все начиналось?..

2 января в массовом доступе появилась информация о том, что практически все процессоры Intel, выпущенные с 1995 года, сделаны с браком. Его назвали модным толерантным словом «уязвимость». Уязвимости, получившие названия **Meltdown** («Расплавление») и **Spectre** («Призрак», общее название для еще двух уязвимостей), были найдены командами Google Project Zero и Грацского технического университета еще в июне 2017 года. Правда, в Intel заявили, что выявленные ошибки «не могут повредить, изменить или удалить данные пользователей», но на масштабы скандала это не повлияло.

Если говорить проще, то все процессоры Intel включают ошибку проектирования. Эта ошибка может позволить вирусам, шпионским программам и иному вредоносному ПО читать те области памяти ядра, которые до сих пор считались защищенными от незаконного вторжения. Например, область ОЗУ, выделенная для наиболее важных основных компонентов операционной системы и их взаимодействия с системным оборудованием.

> Корень проблемы - так называемое спекулятивное исполнение команд, то есть технология в современных микропроцессорах, позволяющая «предугадывать», какие команды потребуется исполнить в будущем. К примеру, программа А выполняет сложную математическую операцию, в ходе которой будет использована сумма каких-то переменных. Программа В заранее (когда процессор менее нагружен) считает эту сумму, чтобы ускорить работу процесса в будущем, и в нужный момент подсовывает результат программе А. Эти действия производятся во внутренней памяти процессора на нескольких слоях кэша (в зависимости от архитектуры). Уязвимость спекулятивного исполнения заключается в том, что злоумышленники могут получить доступ к данным, которые находятся в этой общей памяти.

Таким образом, для хакеров в вашем компьютере больше нет совершенно закрытых мест. Используя уязвимости в процессоре, они теоретически могут залезть в любой компьютер, пройтись по всем данным и взять то, что им захочется. Ошибка внесена на аппаратном уровне 64-битных процессоров Intel, и поэтому она

требует исправления на базовом уровне в каждой популярной операционной системе, включая Windows, Linux и macOS.

Величина проблемы пока не раскрывается, но, если учесть, что разработчики всех уровней забыли про рождественские и новогодние каникулы и изо всех сил уже больше полугода работают над программными «заплатками», чтобы выпустить обновления в ближайшие дни, можно предположить, что ситуация серьезная.

Уже известно, что «заплатки» повлекут за собой полное разделение памяти ядра и пользовательских процессов. Исправления, названные KPTI (Kernel Page Table Isolation), переносят ядро ОС в полностью отдельное адресное пространство. Вот только проблема такого разделения памяти состоит в том, что поддерживать переключение между двумя отдельными адресными пространствами для каждого системного вызова и для каждого аппаратного прерывания очень ресурсозатратно. Такие переключения заставляют процессор выгружать кешированные данные и заново загружать информацию из оперативной памяти, что увеличивает расходы ресурсов на работу ядра ОС.

Таким образом, «исправленные» операционные системы потенциально могут привести к значительному падению производительности компьютеров — от 5% до 30%, в зависимости от конкретной задачи и модели процессора. В условиях личных компьютеров это практически никак не скажется на работе или отдыхе пользователя – могут только «подвисать» некоторые страницы интернета или высокопроизводительные игрушки. А вот в масштабах больших центров по обработке данных ухудшение производительности процессора может привести к серьезным последствиям.

> Уязвимость Meltdown позволяет нарушить барьер между приложениями и внутренней памятью операционной системы. Это открывает доступ к данным, хранимым в памяти ОС. Spectre нарушает такой барьер между самими приложениями – то есть, один сервис может залезть в память другого. Это более сложная атака, и она еще некоторое время будет угрожать пользователям.

Ладно Intel – а что с другими?

Meltdown подвержены практически все процессоры, выпущенные компанией Intel с 1995 года (кроме моделей Intel Itanium и Intel Atom, выпущенных до 2013 года). Spectre же касается не только процессоров Intel, но и AMD и ARM (семейства Cortex-A и Cortex-R) – а это не только ПК, но и ноутбуки, планшеты и смартфоны. При этом следов вторжения Meltdown и Spectre не оставляют — пользователи вряд ли смогут определить, украли ли у них данные.

Компания AMD — прямой конкурент Intel. Процессоры этого производителя часто используются в персональных компьютерах. ARM производит чипы для мобильных устройств. В ARM заявили, что обнаруженные проблемы касаются некоторых процессоров серии Cortex-A, а вот чипы серии Cortex-M, используемые в устройствах «интернета вещей», не подвержены уязвимости.

В компании AMD вообще говорят о «почти нулевом риске», но работа над поиском новых уязвимостей еще ведется, и поэтому все может измениться.

Исследователи из Google Project Zero утверждают, что уязвимость Meltdown пока подтверждена только на чипах Intel, а вот вторая уязвимость касается процессоров абсолютно всех производителей.

Apple подтвердила, что уязвимость есть на всех компьютерах и смартфонах, произведенных компанией. Google уверяет, что уже устранила все уязвимости во всех своих продуктах и не только: компания опубликовала технические инструкции по защите от потенциальных атак с помощью Meltdown и Spectre.

Что нас ждет

Кражей паролей обычного пользователя в 2018 году напугать сложно. Если это, конечно, не пароль от банковской карты – а его тоже легко можно украсть. Такую возможность дает Meltdown: одно приложение в реальном времени видит через внутреннюю память системы, что вводится в другое приложение. И ваша карточка – уже не ваша.

Для того, чтобы обезопасить себя, нужно установить обновление. Microsoft, и Apple уже выпустили такие

обновления для своего программного обеспечения. При версии Windows ниже 10 придется скачать и установить обновление вручную, а для «десятки» обновления должны были установиться автоматически с 4 января. Это на треть замедлит общую работу компьютера, но коснется только тех задач, которые интенсивно используют процессор.

Отказаться от автоматической установки патчей не получится. Системы будут обновляться автоматически после 9 января. Также все обновления будут устанавливаться на оборудовании «облачных» сервисов, таких, как Amazon Web Services и Microsoft Azure. Резкое падение производительности может привести к отказу работы систем и даже к потере данных пользователей, хранящихся в «облаках».

Meltdown можно просто остановить патчем, а вот со Spectre ситуация сложнее. Для того, чтобы справиться с этой уязвимостью, придется полностью изменить структуру современных процессоров. И для пользователей – выбросить старый процессор и поставить на его место новый. А сколько этот новый будет стоить – даже не вопрос…

Google обещает к 23 января выпустить обновление браузера Chrome, которое автоматически устранит уязвимости. А всех пользователей устройств на базе ОС Android Google успокаивает тем, что на «большинстве Android-устройств уязвимость сложно воспроизводима и ограничена».

Можно также отказаться от использования обновления и подвергать свои данные риску.

Известно ли об успешных атаках настоящих злоумышленников с применением Meltdown и Spectre? Пока нет.

> Насколько это страшно – покажет время. Вот только глава Intel Брайан Кржанич в ноябре 2017 года продал принадлежавший ему значительный пакет акций компании. Он прекрасно знал об обнаружении неполадок, хотя официальный представитель Intel заявляет сейчас, что сделка проводилась в рамках заранее утвержденного плана. Вот только план был составлен 30 октября, а данные о нахождении уязвимостей компания получила в июне…

Автор: Алина Саратова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 3700 07.01.2018, 13:58
14
URL: https://babr24.com/?IDE=272687 Bytes: 8685 / 8322 Версия для печати Скачать PDF

Автор текста: **Алина Саратова**.

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта