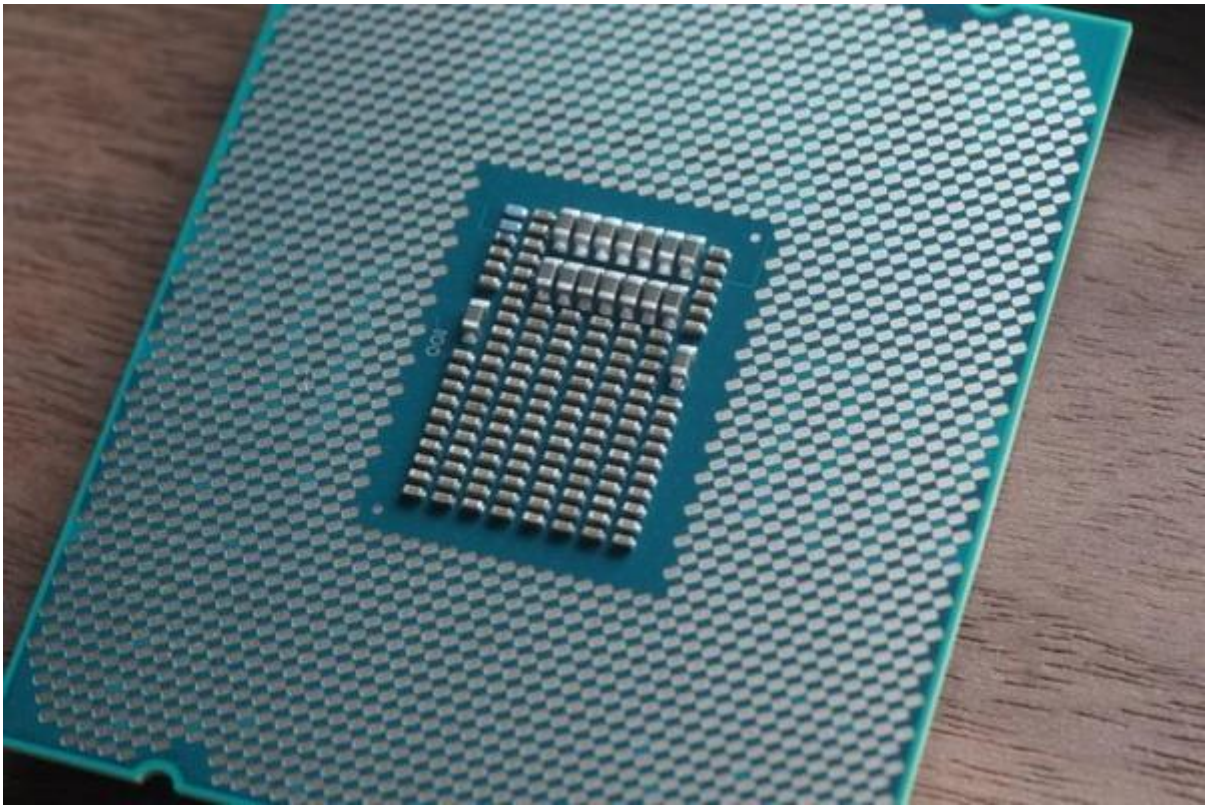
Intel обещает заплаты, обеспечивающие процессорам иммунитет к эксплойтам Meltdown и Spectre



Источник: Intel

12:07 06.01.2018

Бреши были обнаружены специалистами по безопасности из Google. В Intel признались, что были в курсе их существования еще с июня 2017 года, и планировали объявить о них в ближайшие недели, когда будут готовы заплаты.

В Intel заявляют, что уже в ближайшее время предложат заплаты для 90% ее процессоров, выпущенных за последние пять лет, придающие ПК и серверам «иммунитет» к эксплойтам, которые используют бреши Meltdown и Spectre. Заплаты предоставляются в форме обновлений микропрограмм и операционных систем.

Обе бреши связаны с особенностями реализации упреждающего выполнения команд — методики, призванной ускорить работу процессора за счет выполнения инструкций еще до того, как это понадобится программе. Для использования возможностей упреждающего выполнения программе требуется доступ к закрытой области памяти, в которой могут находиться пароли доступа, данные по банковским картам и т. п. Обе бреши позволяют

злоумышленнику считать данные из этой области, когда к ней обращается программа. Meltdown позволяет написать эксплойт, крадущий конфиденциальную информацию, но данную брешь можно обойти с помощью программной заплаты. В свою очередь эксплойты, использующие Spectre, могут считывать память других программ, работающих параллельно с ними, и устранить эту брешь гораздо сложнее.

Впервые бреши были обнаружены специалистами по безопасности из группы Google Project Zero. В Intel признались, что были в курсе существования уязвимостей еще с июня 2017 года, и планировали объявить о них в ближайшие недели, когда будут готовы заплаты для большинства систем. Однако ввиду того, что ряд изданий во главе с The Register уже опубликовали сообщения о Meltdown и Spectre, корпорации пришлось распространить официальное подтверждение раньше.

В частности, корпорация опубликовала список своих чипов, подверженных уязвимости: это Core i3, Core i5, Core i7 и чипы семейства Core M (45 и 32 нм); процессоры Core со 2-го по 8-е поколение включительно; чипы серии Core X для платформ Intel X99 и X299; Xeon серий 3400, 3600, 5500, 5600, 6500, 7500; семейства Xeon E3 и E3 v2-v6, E5 и E5 v2-v4, E7 и E7 v2-v4; Xeon Scalable; Xeon Phi серий 3200, 5200 и 7200; Atom серий C, E, A, x3, Z; а также Celeron и Pentium серий J и N.

В Intel утверждают, что уязвимости касаются не только ее процессоров, но также продуктов ARM Holdings и AMD, о чем эти компании уведомлены. Есть и другие поставщики, чьи продукты уязвимы для тех же эксплойтов, в том числе ряд разработчиков операционных систем, добавляют в корпорации.

В AMD, однако, заявляют, что риск для ее процессоров «близок к нулевому». Компания опубликовала таблицу, согласно которой один из трех способов использования бреши, найденных специалистами Google, блокируется с помощью «обновления ПО или ОС с пренебрежимо малым влиянием на производительность», а два других неработоспособны «ввиду архитектурных отличий процессоров AMD».

В ходе селекторного совещания, посвященного бреши, в Intel отметили, что реальные атаки, использующие уязвимость, на сегодня неизвестны. В корпорации также отрицают, что брешь связана с каким-либо конструктивным дефектом процессоров, заявляя, что ее чипы «работают так, как их спроектировали».

Что касается заплат, для Windows исправление, защищающее от эксплойтов Meltdown, вышло еще 3 января; обновления микропрограмм для большинства чипов Intel уже доступны на сайте корпорации; Apple выпустила обновление macOS High Sierra 10.13.2 с необходимыми заплатами 6 декабря; а хромбуки получили защиту 15 декабря с выпуском Chrome OS 63. Существует также метод обхода бреши для браузера Chrome, а разработчики остальных браузеров готовят исправления.

В первоначальных сообщениях о Meltdown и Spectre утверждалось, что программные заплаты против этих уязвимостей способны замедлить работу приложений на 5-30% в зависимости от задачи. В Intel, однако, утверждают, что приложения, работающие в пользовательском пространстве, замедлятся не более чем на 2%. В PC World, проведя тесты на ряде популярных игр, сообщают, что существенного снижения частоты кадров заплаты для Linux и Windows не вызывают. В то же время сообщается, что некоторые приложения, особенно системы виртуализации, облачные нагрузки и задачи центров обработки данных могут пострадать сильнее.