Ученые из Швейцарии обнаружили новую уязвимость в процессорах Intel, связанную с функцией прогнозирования команд. Эта технология позволяет ускорять работу компьютеров, предугадывая, какие действия нужно выполнить следующими. Но именно она стала причиной очередной проблемы с безопасностью.

Уязвимость обнаружили специалисты из группы COMSEC при ETH Zurich. По их данным, с ее помощью злоумышленник может получить доступ к данным другого пользователя, если оба используют один и тот же процессор. Это особенно актуально для облачных сервисов, где многие клиенты работают на одном оборудовании.

Ошибка получила название BPRC и возникает на уровне процессора в те доли секунды, когда он переключается между задачами пользователей с разными уровнями доступа. При определенной последовательности действий это позволяет получить доступ к данным, хранящимся во временной памяти — кэше и оперативной памяти.

Атака работает не сразу — за один раз можно получить лишь один байт информации, но процедуру можно повторять быстро и читать память со скоростью до 5000 байт в секунду. Это означает, что при достаточном времени можно вытащить весь объем данных.

Проблема выявлена еще в сентябре 2024 года. Intel уже начала внедрение защитных мер через обновления BIOS и операционных систем. Однако исследователи считают, что сама архитектура процессоров с функцией спекулятивного исполнения остается уязвимой и требует глубокой переработки.