Spectre

A falha chamada spectre ocasionou num prejuízo as fabricantes de processadores. Essa falha existem em uma otimização estrutural do chip, o que causa um mal desempenho. É uma falha bastante de corrigir, tendo em vista que seria necessário que os chips fossem reprojetados, ou seja, redesenhar todos os componentes para solucionar o caso. O spectre está relacionado a execução especulativa, que para acelerar o desempenho dos softwares os processadores tentam adivinhar qual código será executado em seguida, descartando aquele código caso a previsão seja errada, causando uma economia de energia.

O spectre quebra o isolamento de duas aplicações diferentes, permitindo com que o invasor engane um programa sem apresentar erros. A falha permite fazer um programa roubar e até vazar informações de outro, desde que estejam rodando no mesmo sistema. Isso se dar porque o spectre usa a execução especulativa para injetar um código malicioso que também insere um comando para fazer com que o processador adivinhe uma informação especifica que não seria executada normalmente, mas por conta do design, ele retorna um comando para um determinado programa quebrando a segurança dos softwares, permitindo com que o invasor fique à vontade para pegar o que quiser sem sabermos, pois é difícil identificar se o programa que está sendo rodado apresenta problemas.

Não só processadores Intel, mas também da AMD e até os núcleos que envolve a arquitetura da ARM, somado a isto temos também temos o Nintendo Switch que usa CPU octa-core com núcleos ARM, todos esses dispositivos são vulneráveis, quanto ao Xbox One e o PS4 é um caso à parte dos vídeo games, pois utilizam CPUs jaguar da AMD que é diferente quanto a sua arquitetura. O estrago que causaria nos usuário domésticos, ou gamers seria até leve em comparação a grandes empresas como a GOOGLE e a APPLE que teriam risco de ter não só os dados da empresas vazados como também de seus usuários.

Para solucionar o problema a Intel lançou sua nona geração de processadores, que apresenta mudanças de hardware para ser imune ao spectre e suas variantes, como é o caso da variante Bounds check Bypass (spectre variante 1) que era a mais complicada de se resolver, pois teria que mudar a arquitetura dos processadores, o que dá muito trabalho, e as soluções vem sempre com a ajudar das atualizações, e as correções do hardware da 9º geração não afetaria o desempenho dos novos processadores. Mas nem todos os modelos de processadores vem com essa solução, mas para a proteção terá updates de firmware.