Spectre: a falha que afeta todo mundo

O Spectre é uma falha mais difícil de corrigir, porque, para ser totalmente resolvida, exigiria que os chips fossem reprojetados. Sim: há uma falha de design em quase todos os processadores modernos do mercado. No entanto, as empresas já trabalham para mitigar o problema por software.
O nome do Spectre está relacionado à causa do problema, que é a execução especulativa (speculative execution, em inglês). Para acelerar o desempenho dos softwares, os processadores modernos tentam adivinhar qual código será executado em seguida. Caso a previsão esteja errada, o resultado é simplesmente descartado; caso esteja certa, há uma economia de tempo aqui.
No entanto, a tecnologia também pode induzir um processador a executar uma operação "adivinhada" que não seria executada em condições normais. Isso permite que um aplicativo vaze uma informação confidencial para outro aplicativo, quebrando vários mecanismos de segurança de softwares, como o sandbox do Chrome, que separa as abas de sites e o resto do sistema operacional, por exemplo.
A Intel divulgou um comunicado afirmando que tem conhecimento do problema, mas ressaltou que as brechas não estão restritas a seus chips, citando nominalmente a AMD e a ARM. Diz ainda que "qualquer impacto no desempenho depende da carga de trabalho e, para o usuário comum, não deve ser significativo".
A AMD admitiu que seus chips são vulneráveis, mas em uma escala menor. "A ameaça e a resposta às três variantes diferem de acordo com a fabricante do processador, e a AMD não é suscetível a todas as três variantes. Devido às diferenças na arquitetura da AMD, acreditamos que existe risco quase zero para os processadores da AMD neste momento".
Em novo comunicado, a AMD informa que não está sujeita ao Meltdown; uma das variantes do Spectre têm risco quase zero de ser explorada nos chips da marca, devido às diferenças de arquitetura; e outra variante do Spectre poderá ser mitigada por correções de software, com "impacto insignificante na performance".
A ARM confirma que alguns núcleos Cortex-A (A8, A9, A15, A17, A57, A72, A73 e A75), utilizados principalmente em smartphones com chips da Qualcomm, MediaTek e **Samsung**, são afetados, mas não os Cortex-M, focados em internet das coisas. O método "requer um malware rodando localmente e pode resultar em dados sendo acessados de uma memória privilegiada", segundo a ARM.

referencia do artigo:
https://tecnoblog.net/231300/meltdown-spectre-intel-amd-arm-falha-processadores/ acesso 11/10/2018