As falhas Spectre existem em uma otimização estrutural do funcionamento do chip. E a correção é feita via software onde faz o que os processadores que receberem essa correção chegue a ter alta perda de desempenho de processamento. Spectre é uma falha relacionada a uma técnica de predição de código a ser executado, com o intuito assim de ter uma alta performance, e a falha se dá nesse meio.

Essa falha permite com que hackers possam ter acessos à partes da memória que não seria permitido, mas para tal coisa o hacker deveria já está dentro do sistema.

Esse acesso a memória indevida, seria como acessar dados de um outro programa de outro usuário. Como o serviço da Amazon, Amazon Web Service que faz com que um computador seja utilizados por vários usuários de forma isolada, com essa falhar um usuário poderia ter acesso à dados de outros usuários.

“De acordo com a Heise, é exatamente nesse cenário que as falhas da Spectre-NG são mais perigosas. Diferente da Meltdown, a falha Spectre original era notória por ser bem difícil de explorar, o que tem mantido alguns ataques mais graves na teoria.”

http://g1.globo.com/tecnologia/blog/seguranca-digital/post/intel-esta-corrigindo-novas-versoes-da-falha-spectre-diz-site.html

Apesar da ser falhar graves a correção não é tão complicada, feita via software, mas em alguns processadores perderia poder de processamento significativos.