Falha Spectre

Em janeiro de 2018 foi anunciada uma falha de segurança gravíssima nos processadores da intel, que ficou conhecida pelo nome spectre, essa falha não se relaciona com alteração em dados, porém permite a espionagem deles. Os responsáveis por possibilitarem essa descoberta foram os membros do Google Project Zero (analistas de segurança da google), pesquisadores das Universidades de Graz na Áustria, maryland e Pensilvânia nos EUA e Adelaide na Austrália e também pesquisadores da Cyberus e Rambus (companhias de segurança).

O Spectre interrompe o isolamento entre diferentes aplicativos, permitindo um ataque que engana programas e ocorre livre de erros, seguindo as melhores formas de encontrar dados e permitir vazamento. Na realidade, as verificações de segurança aumentam a superfície de ataque e podem tornar os aplicativos mais suscetíveis ao Spectre. Os ataques do Spectre envolvem a indução de uma vítima a realizar especulativamente operações que não ocorriam durante a execução correta do programa e que vazam as informações confidenciais da vítima através de um canal lateral.

Um programa mal-intencionado pode explorar o Spectre para se apossar de segredos armazenados na memória de outros programas em execução. Isso pode incluir senhas armazenadas em um gerenciador de senhas ou navegador, fotos pessoais, e-mails, mensagens instantâneas e até mesmo documentos. É sabido que quase todos os sistemas são afetados pelo Spectre: Desktops, notebooks, servidores em nuvem e Smartphones. Mais especificamente, todos os processadores modernos capazes de manter muitas instruções são potencialmente vulneráveis. Foi encontrado o Spectre em processadores Intel, AMD e ARM.

Felizmente a intel lançou correções para o problema spectre, porém as correções não abrangem todos os processadores e logo nas primeiras versões de correção os usuários relataram diversos problemas, como redução no desempenho do processador (devido a correção via software) e tela azul.

Aluno: Rodrigo de Andrade Rolim Bem.