MELTDOWN AND SPECTRE

Por: Débora Bianca Taveira de Moura

Em 2018 uma grave falha de segurança em chips da Intel, ela permite que um aplicativo comum possa acessar áreas protegidas da memória do sistema operacional. Há também brechas que afetam processadores da AMD, da ARM e de muitos computadores e servidores pelo mundo.

As vulnerabilidades são conhecidas como Meltdown e Spectre, elas foram reportadas à Intel, AMD e a ARM em junho, mas só se tornaram públicas esse ano.

MELTDOWN

Essa vulnerabilidade consiste em quebrar um mecanismo de segurança dos processadores, até agora se restringe à processadores Intel, que previne que qualquer aplicativo (comum, ou malware, ou um código em JavaScript executado no navegador) acesse a parte da memória que é reservada ao kernel do sistema operacional. A falha é considerada grave. Todavia, a correção já está sendo implementada para todos os sistemas operacionais.

SPECTRE

O nome é baseado em sua origem. Por não ter uma solução simples irá assombrar por um tempo os usuários e desenvolvedores. É uma falha tanto no design do processador quanto no software, nesse caso a correção dela se torna mais difícil de ser corrigida.

Desktops, notebooks, servidores em nuvem, e smartphones são afetados pelo spectre, mais especificamente, todos que possuem processadores modernos são potencialmente vulneráveis.

Para acelerar o desempenho dos softwares, os processadores mais recentes tentam prever qual código será executado, e caso esteja certo, há uma economia de tempo. O spectre no caso, induz o processador a executar uma operação que não será executada em condições normais, isso faz com que um aplicativo vaze informações confidenciais para outro aplicativo, quebrando vários mecanismos de segurança de softwares.

REFERÊNCIAS

Meltdown and Spectre: https://meltdownattack.com/

Tecnoblog - Meltdown e Spectre:
https://tecnoblog.net/231300/meltdown-spectre-intel-amd-arm-falha-processadores/