Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Redes do Governo

Alerta de Vulnerabilidade nº 01/2018 – Vulnerabilidade em Arquitetura de CPU

1. Descrição do Problema

Pesquisadores identificaram que as implementações de CPU da Intel, AMD e ARM, são vulneráveis a ataques de canal lateral. Essa vulnerabilidade foi categorizada em dois ataques, denominados Meltdown (CVE-2017-5754) e Specter (CVE-2017-5753 e CVE-2017-5715). Esses ataques são descritos em detalhes pelo Google Project Zero e pelo Instituto de Processamento e Comunicação de Informação Aplicada (IAIK) da Graz University of Technology (TU Graz).

2. Possíveis Riscos

Esses ataques são possíveis devido à interação entre o gerenciamento da memória do sistema operacional e a otimização da implementação da CPU. A execução especulativa* e a implementação de cache** permitem que um invasor leia a memória do kernel, com isso o atacante será capaz de executar código com privilégios de usuário, permitindo a recuperação de informações que podem levar a um bypass de KASLR (Kernel Address Space Layout Randomization), dando acesso a dados confidenciais da vítima.

* www.ic.unicamp.br/~ducatte/mo401/1s2006/T2/050269-T.pdf

** https://www.quora.com/What-is-smart-cache-introduced-in-Intel-processors

3. Dispositivos afetados

AMD, Android, Apple, ARM, Chrome, Firefox, Google, Intel, Linux, macOS, Meltdown, Microsoft, Spectre, Windows

4. Sugestões para Mitigação do Problema

- Aplique as correções conforme orientação do fabricante (**No entanto, a correção atual poderá causar instabilidade, lentidão e/ou paralização do Sistema**).
  - WINDOWS: https://tecnoblog.net/231319/microsoft-windows-10-correcao-meltdown-spectre/).
  - LINUX: https://www.cyberciti.biz/faq/patch-meltdown-cpu-vulnerability-cve-2017-5754-linux/
  - REDHAT: https://access.redhat.com/security/vulnerabilities/speculativeexecution
  - APPLE: http://appleinsider.com/articles/18/01/03/apple-has-already-partially-implemented-fix-in-macos-for-kpti-intel-cpu-security-flaw
  - ANDROID: https://support.google.com/faqs/answer/7622138
- Por fim, realize campanhas internas, alertando os usuários sobre esta publicação.

5. Referências

- http://www.kb.cert.org/vuls/id/584653

Brasília-DF, 04 de janeiro de 2018.
Equipe do CTIR Gov