Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Alerta de Segurança 001/2018 –Cogetic/VPGDI

Em 8 de janeiro de 2018

Para: Gestores de TI das unidades da Fiocruz

Assunto: Vulnerabilidades Meltdown e Spectre

Prezados Gestores de TI da Fiocruz, encaminhamos Alerta de Segurança sobre vulnerabilidade em arquitetura de CPU.

Descrição do problema

Vulnerabilidades críticas foram descobertas e reveladas por pesquisadores do Google Project Zero e pelo Instituto de Processamento e Comunicação de Informação Aplicada (IAIK) da Graz University of Technology (TU Graz), sobre implementações de CPU da Intel, AMD e ARM, caracterizados em dois ataques: Meltdown (CVE-2017-5754) e Spectre (CVE-2017-5753 e CVE-2017-5715). Essas vulnerabilidades sujeitam os processadores à ataques de canal lateral.

Descrição dos ataques

O Meltdown pode permitir que hackers ganhem acesso privilegiado a partes da memória usada por programas e aplicações e o Sistema Operacional. O Meltdown afeta, em princípio, processadores Intel.

O Spectre pode permitir que atacantes roubem informações vazadas no kernel ou dados armazenados na memória de programas em execução (credenciais, por exemplo). O Spectre afeta processadores Intel, AMD e ARM.

Os processadores modernos implementam um recurso chamado “execução especulativa”, que permite ao processador especular algumas funções que provavelmente ocorrerão em seguida. Ao armazenar essas especulações, eles otimizam o processamento dos dados e executam as tarefas mais rapidamente. Porém, essa técnica também permite acesso aos dados que deveriam estar isolados, possibilitando a um atacante enviar um *exploit* que, em tese, poderá acessar dados sigilosos.

Impactos

Embora tenham a mesma base, as duas falhas têm impactos e método de exploração diferentes, variando de acordo com o modelo do processador. A falha Meltdown, em princípio, está restrita a processadores Intel. A Spectre, embora exista em outros chips, é considerada de mais fácil exploração em chips da Intel.

O impacto potencial é grande, afetando desktops, laptops e smartphones rodando em processadores vulneráveis e que podem estar expostos a acesso não autorizado e roubo de informações. Servidores, nuvem, ambientes virtuais, appliances corporativos, ou qualquer outro dispositivo que funcione com base nesses processadores também está impactado.

Recomendações

Embora ataques ainda não tenham sido presenciados, provas de conceito evidenciam seu potencial ofensivo. Desta forma, é vital que, na medida em que correções sejam disponibilizadas, essas sejam testadas e implementadas a fim de mitigar os possíveis riscos. É importante estar ciente que as correções existentes podem causar instabilidade, lentidão e/ou paralização do sistema. Abaixo, seguem informações de alguns fabricantes sobre as correções:

- 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-fixin-macos-for-kpti-intel-cpu-security-flaw
- ANDROID: https://support.google.com/faqs/answer/7622138

Referências

- http://www.kb.cert.org/vuls/id/584653
- http://www.ctir.gov.br/arquivos/alertas/2018/ALERTA_2018_01_ArquiteturaCPU.pdf

- https://mobile.nytimes.com/2018/01/03/business/computer-flaws.html?referer=https://t.co/p1JhdWSzln?amp=1
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5753
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754
- https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715
- https://realprotect.net/blog/notificacao-de-seguranca-vulnerabilidades-meltdown-e-spectre/
- https://medium.com/security-thoughts/bem-vindo-ao-cyberggedon-o-apocalipse-dos-processadores-é-muito-pior-do-que-você-imagina-45f24f1adf91
- https://tecnoblog.net/231462/google-retpoline-spectre-meltdown-falha-processador/
- https://tecnologia.uol.com.br/noticias/redacao/2018/01/04/patch-do-windows-10-para-evitar-falha-em-processadores-gera-mais-problemas.amp.htm?__twitter_impression=true

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações