Boletim de Segurança 001/2018

Falha de Segurança em Processadores

Data: 2018-01-03

Última atualização: 2018-01-23| 16:40

Estado: em investigação.

Sumário

Foram publicadas no dia 03/jan/2018 falhas de segurança (Meltdown e Spectre) em vários processadores (Intel, AMD, ARM, Qualcomm, NVIDIA) que permitem explorar áreas de memória protegidas do kernel.

Nota importante

A Intel a recomendou a 22/jan suspender todas as atualizações firmware até novas indicações.

Descrição

As falhas agora publicadas permitem explorar áreas de memória protegidas do kernel em vários processadores (ainda em identificação de todos os modelos afetados), acedendo à informação aí armazenada.

Ainda não são conhecidos *exploits*, nem correções definitivas.

As falhas estão reportadas sob os identificadores CVE (Common Vulnerabilities and Exposures):

- CVE-2017-5715
- CVE-2017-5753
- CVE-2017-5754

Produtos afetados

A informação disponível indica que são afetados, pelo menos, os seguintes produtos:

- Processadores Intel, AMD, ARM, Qualcomm, NVIDIA,…;
- Sistemas Operativos Microsoft, Linux, MacOS, ChromeOS, IOS, Android, tvOS,…

Recomendações

Não existem ainda soluções definitivas, no entanto, os vários fabricantes têm lançado atualizações que pretendem mitigar o risco de ataque.

Existe uma ferramenta disponibilizada pela Intel que verifica se computador está vulnerável.

Importante: Ver Computadores com processador AMD, depois do uptate, não fazem boot.

Sistemas operativos

Clientes Microsoft

Utilizadores Finais (informação não técnica)

Atualizar os Sistemas: **Start → Settings → Update & security → Windows Update → Check for updates**

- Manter os sistemas operativos e as aplicações (com especial destaque para os antivírus) atualizados.
- Manter o firmware dos computadores e dispositivos atualizados.

Técnicos (informação técnica)
https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in

Sistemas Servidores Microsoft

Sistemas Linux RedHat

Sistemas Linux UBUNTU

Sistemas Apple

Hardware:

Acer

Asus

Cisco

Dell: Clientes | Servidores

HP

Lenovo

Antivírus

Windows antivírus patch compatibility

Referências

https://spectreattack.com/

https://googleprojectzero.blogspot.pt/2018/01/reading-privileged-memory-with-side.html

Agradecimentos

Ao esforço de toda a comunidade que, através das redes sociais, garante uma atualização constante da informação e do feedback dos fabricantes.

Exoneração de Responsabilidade

A Universidade de Aveiro não se responsabiliza por eventuais incorreções na informação ou documentação existente nesta nota técnica, nem pelo conteúdo das páginas para as quais remetem os links ou hiperlinks dele constantes.