-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

CAIS-ALERTA [04/01/2018]: Vulnerabilidade crítica em processadores de diversos fabricantes

Prezados,

O CAIS alerta para vulnerabilidades críticas envolvendo diversas linhas de processadores de vários fabricantes, tais como Intel, AMD e ARM.

DESCRIÇÃO

Vulnerabilidades existentes nas funções de manipulação de dados e memória dos processadores podem permitir o vazamento de informações e/ou execução arbitrária de códigos.

De forma geral, uma aplicação não pode acessar dados de outras aplicações em execução dentro de um mesmo ambiente, porém, programas maliciosos podem explorar falhas nas funções dos processadores e assim obter dados contidos na memória referentes a outros programas em execução.

SISTEMAS AFETADOS

Segundo os pesquisadores responsáveis pela descoberta, grande parte dos processadores modernos produzidos nas últimas décadas são impactados.

CORREÇÕES DISPONÍVEIS

Até o momento, apenas mitigações em nível de software foram disponibilizadas por diversos desenvolvedores. Sendo assim, elencamos as soluções disponíveis de alguns dos principais desenvolvedores de sistemas do mercado:

- - Linux Fundation

https://lkml.org/lkml/2017/12/4/709

- - Microsoft

https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution-s

https://support.microsoft.com/en-us/help/4073119/windows-client-guidance-for-it-pros-to-protect-against-speculative-exe

- - Red Hat Product Errata RHSA-2018:0010 - Security Advisory

https://access.redhat.com/security/vulnerabilities/speculativeexecution

- - SUSE Blog

https://www.suse.com/c/suse-addresses-meltdown-spectre-vulnerabilities/

- - VMware Security & Compliance Blog

https://blogs.vmware.com/security/2018/01/vmsa-2018-0002.html

- - Xen Security Advisory

http://xenbits.xen.org/xsa/advisory-254.html

IDENTIFICADORES CVE

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

MAIS INFORMAÇÕES

- - Meltdown and Spectre

https://meltdownattack.com/

- - CERT

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

- - MeioBit

http://meiobit.com/378206/meltdown-spectre-falhas-criticas-processadores-intel-amd-arm-quase-todo-mundo-foi-afetado/

- - Intel News Byte - Intel Respond to security research findings

https://newsroom.intel.com/news/intel-responds-to-security-research-findings/

- - AMD Processor Security

https://www.amd.com/en/corporate/speculative-execution

- - ARM Processor Security Update

https://developer.arm.com/support/security-update

- - Microsoft Azure

https://azure.microsoft.com/en-us/blog/securing-azure-customers-from-cpu-vulnerability/

- - Amazon AWS

https://aws.amazon.com/security/security-bulletins/AWS-2018-013/

- - Google Cloud

https://blog.google/topics/google-cloud/what-google-cloud-g-suite-and-chrome-customers-need-know-about-industry-wide-cpu-vulnerability/

- - BleepingComputer

https://www.bleepingcomputer.com/news/security/list-of-meltdown-and-spectre-vulnerability-advisories-patches-and-updates/

- - AppleInsider

http://appleinsider.com/articles/18/01/03/apple-has-already-partially-implemented-fix-in-macos-for-kpti-intel-cpu-security-flaw

- - CVE MITRE

http://www.cve.mitre.org/

- - Qualys Blog

https://blog.qualys.com/securitylabs/2018/01/03/processor-vulnerabilities-meltdown-and-spectre

- - The Register

https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/

- - Security Affairs

http://securityaffairs.co/wordpress/67372/hacking/intel-cpu-design-mistake.html

O CAIS recomenda que os administradores mantenham seus sistemas e aplicativos sempre atualizados, de acordo com as últimas versões e correções oferecidas pelos fabricantes.

Os alertas do CAIS também são oferecidos no Twitter:

Siga @redernp @caisrnp

Atenciosamente,

CAIS/RNP

```
##################################################################
#   CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)     #
#       Rede Nacional de Ensino e Pesquisa (RNP)               #
#                                                              #
# cais em cais.rnp.br    http://www.rnp.br/servicos/seguranca  #
# Tel. 019-37873300      Fax. 019-37873301                     #
# Chave PGP disponivel   https://www.cais.rnp.br/cais-pgp.key  #
##################################################################
```


```
-----BEGIN PGP SIGNATURE-----
Version: OpenPGP.js v1.0.1
Comment: http://openpgpjs.org

wsFcBAEBCAAQBQJaTmvbCRB83qA0uPj0mAAAZFAP/RlSTp2hBhX5vPgMUO/L
pSZK435RgAE5ioFRuMNkqdeiZGo2nmF6QWzsiGgJ0YtdwIa903eW4T0s3xMt
DByHia3ukDLMKv9i81wYjUgpodHAPbfNYhaFjFV3bl2rtnrdLs5bCvwEldBo
yR6RPyQiFxXmIRGpfZWY9/iPSEd/nrF7YA1HN09N2tZZN5cpPtg6X1JyHnf+
IfL+LVmoKwwLKW7meA6xmlC/HSDBmht0OnstU3iLLvsVvEuVx4vzUnMSigUA
ZKJXtaqSZvq8aqUyWQlH5GHGXgCgCHG06YhBrhEE23NE54RlarERHDzaHlYP
fQuYf6yanw9ATuDIvXvD6gUqmT0pBQ6uBIGLANest5LUv8U6C/8h0Y/cseFf
WhJntBHTCW4nYXmBLRfYDnIPMsYZWU+uIFfnzvwAhUXFOuVqwEK68O20z3QR
O0YJd7xpSNb0I6CqNyXM9OJugsoLlaq0YDEU2neZ86LVYjZx8P85+u1C4wfB
GsS8AO3f768864lMwtxSJMeyid7RqEhhN0Ab0/e5B/oirB6HCkD4HoTuAnPL
q0HA3GBKtsvXqFe6PuJ2qT4yYi065C9yydGh+Cmr27JpKISi/ueA+xx6D3rV
6uHu75nqXQcn9iXG6ydpMh27Cs+6JsBKjW0K2Xm4y/j4TKjGocCHbxmCyx2r
Fy/+
=m9as
-----END PGP SIGNATURE-----
```