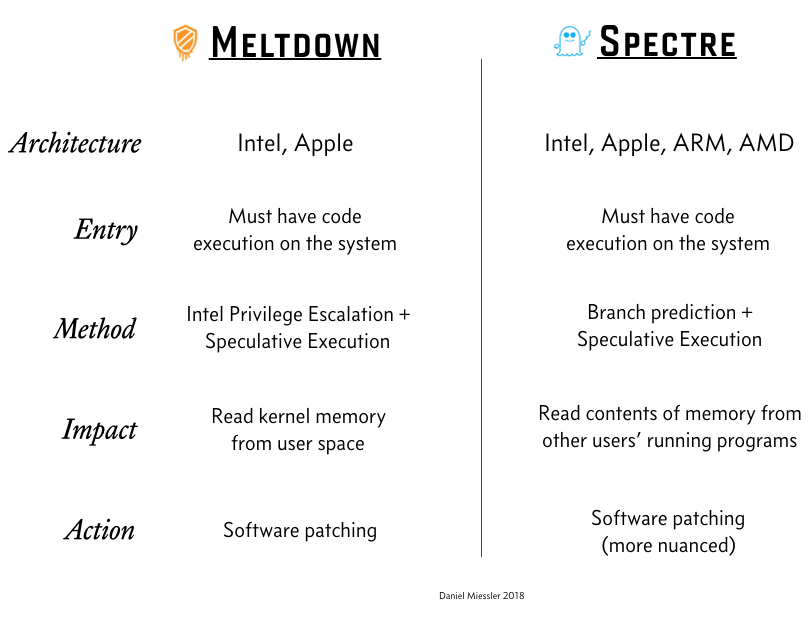
# 漏洞介绍

<http://www.infoq.com/cn/news/2018/01/meltdown-spectre-deep-dive>



Meltdown(熔 断)

相关漏洞：

CVE-2017-5754

介绍：

<http://www.tc260.org.cn/upload/2018-01-16/1516081883218060656.pdf>

熔断漏洞利 用CPU乱序执行技术的设计缺陷，破坏了内存隔离机制，使 恶意程序可越权访问操作系统内存数据，造成敏感信息泄 露。

<https://people.canonical.com/~ubuntu-security/cve/2017/CVE-2017-5754.html>

Systems with microprocessors utilizing speculative execution and indirect

branch prediction may allow unauthorized disclosure of information to an

attacker with local user access via a side-channel analysis of the data

cache.

Amd cpu不受影响

<http://www.amd.com/en/corporate/speculative-execution>

GPZ Variant 3 (Rogue Data Cache Load or Meltdown) is not applicable to AMD processors.

性能影响：

苹果电脑打了补丁后不受影响

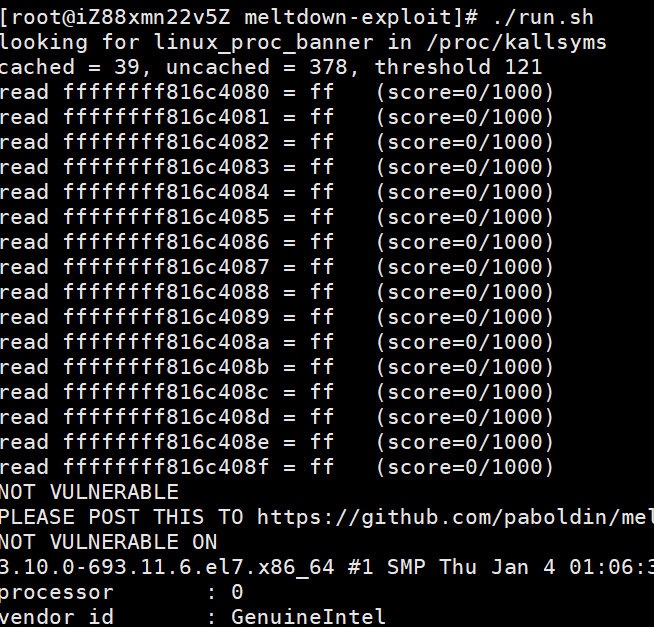
<https://support.apple.com/en-us/HT208394>

Our testing with public benchmarks has shown that the changes in the December 2017 updates resulted in no measurable reduction in the performance of macOS and iOS as measured by the GeekBench 4 benchmark, or in common Web browsing benchmarks such as Speedometer, JetStream, and ARES-6.

漏洞测试：

<https://github.com/paboldin/meltdown-exploit>

图示(使用的云主机,漏洞已经修复)



<https://github.com/IAIK/meltdown>

漏洞修复原理：

使用KAISER来将用户空间和系统空间隔离，同时中断时清空缓存。KAISER在2017年中旬的linux内核中已经自带，但是没有设置为启动。

<https://lwn.net/Articles/738975/>

漏洞修复：

经测试,centos7,centos6,win10的最新补丁已经修复这个漏洞

<http://blog.cyberus-technology.de/posts/2018-01-03-meltdown.html>

KPTI / KAISER Patches

The KPTI / KAISER patches that have already been applied to the latest Linux kernel version help against Meltdown attacks. This series of patches by Gruss et al. ultimately splits user space and kernel space tables by unmapping all kernel memory pages before executing code in user space.

This patch brings a certain amount of performance degradation, but makes Meltdown access to crucial data structures in the kernel impossible.

A similar strategy helps to keep Windows and OS X kernels safe.

Spectre(幽灵)

相关漏洞：

CVE-2017-5753 and CVE-2017-5715

漏洞检测：

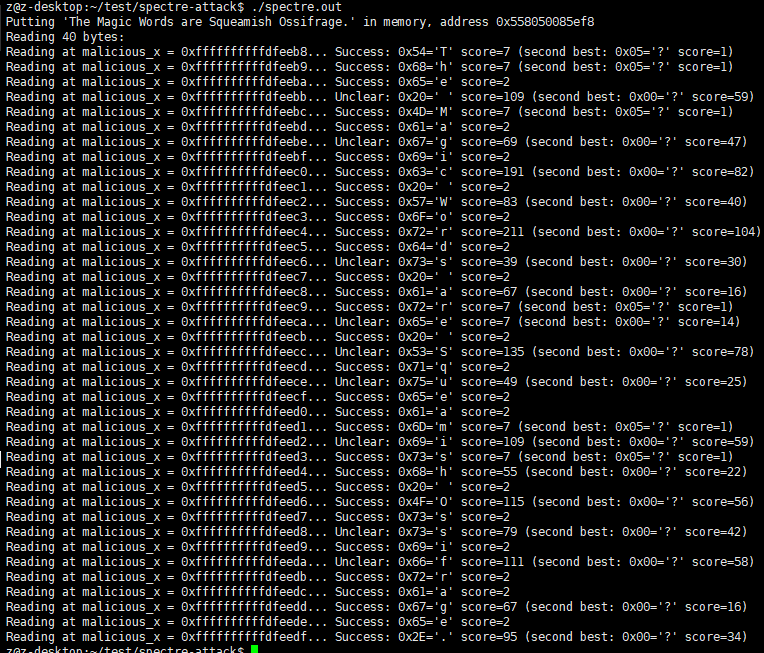
通过javascript检测

<https://react-etc.net/entry/javascript-spectre-meltdown-vulnerability-check-for-browsers>

c检测

<https://github.com/Eugnis/spectre-attack>

图示(使用的云主机,漏洞未修复)



Js测试代码：

<https://react-etc.net/page/meltdown-spectre-javascript-exploit-example>

var TABLE1\_STRIDE = 1;

var TABLE1\_BYTES = 3;

var probeTable = ['alpha', 'beta', 'corky'];

var simpleByteArray = [0x00, 0x01, 0x02];

var localJunk;

var index = 0;

if (index < simpleByteArray.length) {

index = simpleByteArray[index | 0];

index = (((index \* TABLE1\_STRIDE) | 0) & (TABLE1\_BYTES - 1)) | 0;

localJunk &= probeTable[index | 0] | 0;

}

console.log(localJunk);

漏洞介绍：

幽灵漏洞利用了CPU推测执行技术的设计缺陷，破坏了 不同应用程序间的逻辑隔离，使恶意应用程序可能获取其它 应用程序的私有数据，造成敏感信息泄露。

漏洞修复：

截止20180118

CVE-2017-5753

修复需要系统补丁。

CVE-2017-5715

修复需要主板固件刷新和系统补丁

Meltdown & Spectre

性能影响：

<http://www.infoq.com/cn/news/2018/01/meltdown-spectre-deep-dive>

当应用程序进行系统调用让OS内核帮它们做某事时，这些问题补丁的性能影响就会显现出来。为此，Loopback测试可以呈现最坏的情况。Intel[汇总](https://newsroom.intel.com/news-releases/industry-testing-shows-recently-released-security-updates-not-impacting-performance-real-world-deployments/)了来自Apple、Microsoft、Amazon和Google的公告，他们普遍对这些补丁的影响轻描淡写。Cloudflare的CTO [John Graham-Cumming](https://www.infoq.com/profile/John-Graham~Cumming)[表示](https://twitter.com/jgrahamc/status/949252936814747648)，“我们会继续测试#meltdown和#spectre的各种补丁，但对@Cloudflare基础设施的影响似乎可以忽略”。同时，Aeron创建者[Martin Thompson](https://www.infoq.com/profile/Martin-Thompson)[指出](https://twitter.com/mjpt777/status/949262368218984448)，“在Windows上打好Intel的漏洞补丁后，Aeron的良好表现让人意外。系统调用开销增加似乎会导致Aeron批处理增加，进而提高了吞吐量。”，虽然这种情况会影响延时。然而，有人报告了更为严重的性能影响。Syslog\_NG布道师Peter Czanik[发现](https://twitter.com/PCzanik/status/949275491617464320)，在Fedora上，编译时间从4分钟涨到了21分钟（虽然还不如在OpenSUSE上糟糕）。工程部门主管Ian Chan[表示](https://twitter.com/chanian/status/949457156071288833)，“在我们生产环境的部分Kafka代理[d2.xlarge]上，其底层的AWS EC2虚拟机管理程序（大概）已经应用了#Meltdown补丁。CPU增长在5%到25%之间。”

微软补丁：

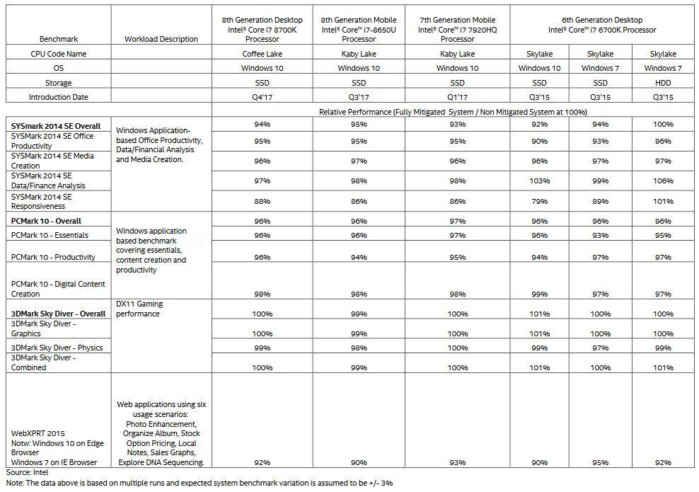
防病毒（AV）软件也有自己的工作要做。目前，微软正在进行检查，确保AV供应商[设置了注册表项](https://support.microsoft.com/en-gb/help/4072699/important-january-3-2018-windows-security-updates-and-antivirus-softwa)，指明应用补丁是安全的，否则，AV可能会试图访问与补丁冲突的内存，导致Windows崩溃。一段时间以后，主机入侵防护系统（[HIPS](https://en.wikipedia.org/wiki/Intrusion_detection_system" \l "Host-based)）（与AV有大量重叠）可能就可以发现利用Spectre的尝试。

<https://newsroom.intel.com/news/intel-security-issue-update-addressing-reboot-issues/>

部分使用Broadwell and Haswell CPU的机器在固件升级后系统重启

性能影响：

<https://www.computerworld.com/article/3247788/computer-hardware/intel-says-new-firmware-patches-trigger-reboots-in-haswell-and-broadwell-systems.html>



一般性能影响5%左右，个别测试影响40%左右

<https://medium.com/implodinggradients/meltdown-c24a9d5e254e>

漏洞介绍：

Project zero

<https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html>

Meltdown and Spectre官网（Graz University of Technology大学主办）

<https://spectreattack.com/#faq-why-meltdown>

微软

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002>

AMD

<http://www.amd.com/en/corporate/speculative-execution>

Apple（已经发放Spectre补丁，ARES-6性能影响2.5%）

<https://support.apple.com/en-us/HT208394>

Ubuntu

<https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SpectreAndMeltdown>

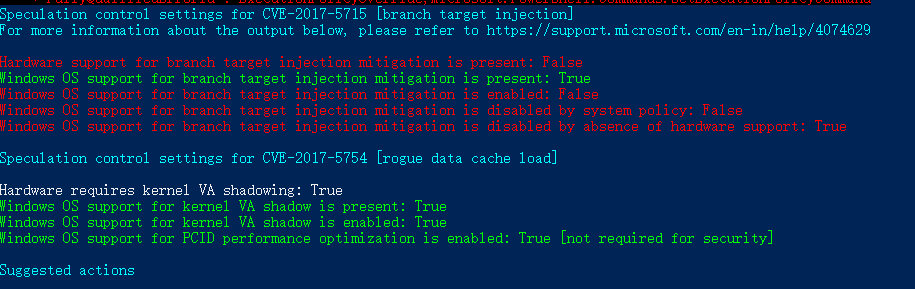
Intel

<https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html>

微软漏洞检测:

<https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in>

图示(使用的办公区电脑，红色部分估计是需要主板固件更新)



QA

1.

防病毒软件可以防止这个漏洞么？

<https://meltdownattack.com>

While possible in theory, this is unlikely in practice. Unlike usual malware, Meltdown and Spectre are hard to distinguish from regular benign applications. However, your antivirus may detect malware which uses the attacks by comparing binaries after they become known.

1. 受Meltdown影响的机器范围

1995年以后的所有Intel的cpu

Desktop, Laptop, and Cloud computers may be affected by Meltdown. More technically, every Intel processor which implements out-of-order execution is potentially affected, which is effectively every processor since 1995 (except Intel Itanium and Intel Atom before 2013). We successfully tested Meltdown on Intel processor generations released as early as 2011. Currently, we have only verified Meltdown on Intel processors. At the moment, it is unclear whether AMD processors are also affected by Meltdown. According to ARM, some of their processors are also affected.

1. 受Spectre影响的机器范围

所有的电脑包括手机

Almost every system is affected by Spectre: Desktops, Laptops, Cloud Servers, as well as Smartphones. More specifically, all modern processors capable of keeping many instructions in flight are potentially vulnerable. In particular, we have verified Spectre on Intel, AMD, and ARM processors.

1. Meltdown和Spectre的区别

都破坏了防止应用任意访问系统内存的机制，最终使应用可以访问系统内存。Spectre可以欺骗其他应用他们的内存。两个攻击都是从获取的内存位置去用旁路去获取信息。

Meltdown breaks the mechanism that keeps applications from accessing arbitrary system memory. Consequently, applications can access system memory. Spectre tricks other applications into accessing arbitrary locations in their memory. Both attacks use side channels to obtain the information from the accessed memory location. For a more technical discussion we refer to the papers ( Meltdown and Spectre)

其他参考：

从理论层面谈Meltdown与Spectre攻击 | 核武按钮终被劫持？

<http://www.freebuf.com/articles/terminal/160424.html>

深入了解Spectre和Meltdown

<http://www.infoq.com/cn/news/2018/01/meltdown-spectre-deep-dive>

关于发布《网络安全实践指南—CPU熔断和幽灵漏洞防范指引》的通知

<http://www.tc260.org.cn/front/postDetail.html?id=20180116090719>

Intel CPU再爆新漏洞：数百万企业级笔记本遭殃

<https://mp.weixin.qq.com/s?__biz=MzU0NDEyODkzMQ==&mid=2247484057&idx=1&sn=57936dbb6882cfc2ecdb85f0cfae6fd4&chksm=fb01a855cc762143aaa8fa187e9171a009edd72551dce56dcb7267847f567f7a4fe71646e7d8&mpshare=1&scene=1&srcid=01147eNyyKWXMgcPaApb1xmt#rd>

英特尔处理器安全性问题 绿盟科技产品及云平台不受影响（附漏洞分析）

<https://mp.weixin.qq.com/s?__biz=MzI2NDI5MTg4MA==&mid=2247485123&idx=1&sn=59a82519f4de00a132c41e56f452dcb9&chksm=eaaf9584ddd81c9237d44a77a25da34c9633ef1ef5ef7e6da26eef1c0a6527535a1c4226283e&mpshare=1&scene=1&srcid=0106zZfqRkceuqS89aG6rMAW#rd>

# WIN SERVER测试报告

## 测试对象

类型：Widows 2008 ， IP：10.129.1.10

类型： widows 2012， IP：10.129.1.11

测试目标

cpu漏洞检测，内存检测

## 修补方式

对测试机进行补丁修复，之后观察cpu， 内存性能情况

## 测试结论

测试机的cpu和内存使用情况和未修补之前没什么区别，查看相关资料进行补充得到下面的主要结论：

1.CPU为2016年及以后且系统是win10时，性能几乎没有影响；

2.系统是win10但CPU是2015及以前的，性能有较大影响；

3.系统是win7/8，CPU是2015及以前的，性能有较大影响；

4.Server系统打补丁后性能都有影响，特别是IO密集型的应用