CPU 漏洞 Meltdown 和 Spectre

1. **技术分析**

Google Project Zero, Reading privileged memory with a side-channel
LWN, Notes from the Intelpocalypse
ARM, Cache Speculation Side-channels

2. **厂商**

	厂商	要点
CPU 提供商	Intel	1. 不是 Intel 一家的问题 2. 性能影响与具体应用负载有关。一般来说不大 3. 积极准备发布修复用的软件和固件。 -- Intel CEO 不久前曾出售公司股票
公有云提供商	Google	1. 安装最新安全更新的 Android 系统不受影响 2. Google Apps / G Suite, 客户无需任何修改 3. Google Chrome, Chrome OS 需要修改设置 4. Google Home / Chromecast, Google Wifi/OnHub 客户无需任何修改 5. Google Cloud Platform 下列服务需要客户更新 - Google Compute Engine - Google Kubernetes Engine - Google Cloud Dataflow - Google Cloud Dataproc
	AWS	1. 大部分 EC2 实例已经得到保护 2. 客户还需要打操作系统补丁 3. Amazon Linux 已经打好补丁， Windows 还得等 Microsoft
	Microsoft Azure	1. 迄今没有任何信息表明客户已经被攻击 2. 大部分已经升级，少部分正在升级且需要重启服务器 3. 高可用 SLA 不变 4. CPU 和 I/O 性能影响不大，少部分客户可能会感受到网络性能下降， 可用 Azure Accelerated Networking 调整
虚拟化及操作系统厂商	VMWare	1. VMware ESXi 受影响， 暂无解决方案 2. Workstation 和 Fusion 最新版无影响
	Red Hat	1. RHEL, Openshift, Openstack 均受影响 2. 修复工作进行中

		3. Protect your Fedora system against Meltdown
	Xen	1. 所有运行 Xen 的系统均受影响 2. 暂无解决方法
浏览器厂商	Google Chrome	1. 开启『严格站点隔离』选项 2. 内存使用会增加 10%-20%， 打印和开发工具不会完全支持跨站点的 iframe
	Mozilla	1. 采用类似技术，可以读取其他源的私有信息 2. 在 Firefox 57 中 - performance.now 减少为 20us - 默认禁止 SharedArrayBuffer

3. 媒体报道

WIRED, A Critical Intel Flaw Breaks Basic Security For Most Computers

Softpedia, Billions of Devices at Risk of Attacks Because of Two Critical Hardware Bugs, These bugs affect all devices made in the last 25 years

Forbes, Massive Intel Vulnerabilities Just Landed -- And Every PC User On The Planet May Need To Update

The Register, Kernel-memory-leaking Intel processor design flaw forces Linux, Windows redesign