芯片漏洞不只是修复那么简单：补丁对性能的影响已经显现；部分企业选择暂缓修复

AngelaY 2018-01-11 共144510人围观，发现 5 个不明物体 观点 资讯

自 **Meltdown** 和 **Spectre** 芯片漏洞曝出以来，**FreeBuf** 已经持续关注、发布了不少相关的报道与分析文章。目前，网很多分析文章的核心都集中在保护处理器速度，这一点的优先级已经超过了安全的考量。就连很多厂商的修复方案以不影响设备性能为核心。

每次有漏洞爆出，厂商发布补丁的速度永远都会被诟病，这次也不例外。针对这两个漏洞，云用户和 IT 管理员尤其注意并及时修复。按理说打完补丁、升级更新就没事儿了。但显然事实没有这么简单，有些不幸的用户遇到了更多烦。

在披露漏洞之后，Google 表示目前已经发布的软件修复程序“造成的性能影响程度最低”，并坚称随着时间的推移，丁对性能的影响还会减轻。而英特尔也在声明中表示：“任何性能影响都取决于工作负载。对于一般的计算机用户来说，补丁对性能的影响并不明显，且随着时间的推移也会减轻”。由于芯片存在所谓的 Processor-Context ID（PCID）处理器特征，这些说辞可能都有道理，最终可能都正确。但其实后续还有更多问题。

补丁对设备性能带来的影响已经显现

虽然大部分普通桌面用户和游戏玩家都没有注意到设备延迟、减缓或者性能下降，但运行 **IO** 或系统调用密集型软（如后端服务器上的数据库）的用户可能会注意到补丁 **CPU** 的影响。

美国红帽公司已经将补丁对性能的影响范围设置为 1% 到 20%。而 Epic Games 也在上周五针对最近玩家登录中遇到问题和服务器稳定性问题做出了解释

> 我们所有的云服务都因为打补丁、修复 Meltdown 和 Spectre 而受到影响。

Epic Games 主要依靠 AWS 服务器运行，他们在声明中发布了一张图表截图，图表显示，主机打完补丁后 CPU 利用一路飙升。

专家还分析了并行分布式文件系统 Lustre 的邮件列表，结果显示，某些 **IO** 密集型应用程序的运行速度都有降低，低程度在 **10**% 到 **45**% 之间。

莱布尼茨波茨坦天体物理研究所的阿尔曼·卡拉蒂坦（Arman Khalatyan）在周一的备忘录中写道：

> 我们在具有 zfs+compression+lustre 的测试系统上发现性能受到严重影响。

在 Reddit 上，一名 Monero 挖矿工人反馈显示，在应用 Meltdown 补丁之后，性能下降了大约 45%。另一名矿工则馈 hash 率降低了 10% 到 15%。

基于 AWS 服务器的 Quora 网站表示，由于 **AWS** 使用了英特尔发布的 **Meltdown** 与 **Spectre** 漏洞补丁，目前服务器经减速。

Blueprint Strategy 公司的数据科学家 Francis Wolinski在 Twitter 上指出，在应用 **Windows 7** 的 **Meltdown** 补丁之后，**Python** 运行速度显著减慢，降低了约**37**%。

而分析公司 Branch Metrics 的工程总监 Ian Chan 也通过推特发声：在将 **Meltdown** 补丁应用于处理其 **Kafka** 实例的 **AWS EC2** 管理程序之后，**CPU** 利用率增加了 **5**% 至 **20**%。

不少亚马逊客户分享了打完补丁后的 CPU 使用率截图，都体现了一定的高峰。上周末，亚马逊证实，针对两个漏洞更新将在一定程度上影响 **AWS** 虚拟机的性能，尽管他们也同时表示“大多数客户的工作负载不高，所以补丁对性能影响并不显著”。

而 9 号，很多微软用户反馈表示，安装 Windows KB4056892 补丁后，系统崩溃。

这些案例中性能下降的数据与此前预测的 5%-30%接近。不过具体变化结果与工作负载和相关技术都有关。

据外媒 The Next Platform 估计，CPU 减速带来的计算价值损失高达每年 60 亿美元。

企业担心影响电脑性能，对安装补丁持谨慎态度

由于目前尚未有确定性的研究结果，很多企业担心修复芯片漏洞可能拖慢电脑运行速度、甚至导致电脑系统崩溃，此决定暂缓安装软件补丁，唯恐适得其反。而微软的补丁导致系统崩溃则证明这些企业的担心并非空穴来风。

网络安全初创公司 Obsidian 联合创始人 Ben Johnson 认为：“如果不进行适当的测试就在所有的电脑上安装补丁，可会导致系统崩溃，结果就是所有员工都无法工作。”

国外一家专门分享新出现的网络威胁相关数据的企业 Financial Services Financial Services Information Sharing and Analysis Center 的首席信息风险主管 Greg Temm 称，银行等金融机构将本周的大部分时间都用于研究电脑系统受漏影响的程度。

> 这些缺陷几乎影响到所有电脑和移动设备，但未被视作“严重”风险，因为还没有证据说明，黑客已经掌握利用这些缺陷的方法。这些漏洞对于系统而言，就像人被诊断了高血压。高血压不是急病，不会突然导致心跳停止，不会要命。

Temm 称，银行正测试补丁程序，看它是否会拖慢电脑运行速度；以及如果会令电脑速度减慢，应该作出哪些改进例如，可以把电脑接入网络，以弥补单台电脑处理器运行速度的不足。

Johnson 称，一些流行的杀毒软件程序与补丁程序不兼容，从而会导致台式或笔记本电脑停止响应并显示“蓝屏死机很多杀毒软件厂商对此的反应是修改旗下产品，以期与更新后的操作系统兼容。微软还表示，只有当 Windows 用户用的杀毒软件的厂商证实补丁不会导致客户电脑崩溃时，才会向该用户提供补丁更新。

英特尔仍认为这些程序更新对电脑性能的影响与电脑工作负载紧密相关。对普通电脑用户而言，这种影响应该不大并且将会随时间推移而逐渐减轻。

政府与安全专家称，尚未看到利用相关芯片缺陷实施的黑客攻击。不过预期随着黑客消化安全缺陷的技术数据，他很可能会利用这几个漏洞开发出新代码，针对访问恶意网站的用户发起攻击。

PCID 是唯一的好消息

说了这么多，唯一的好消息是自 2010 年以来英特尔 x86-64 芯片中的 PCID 功能可以缓解 Meltdown 补丁带来的性能毁。（如果用户的系统是 32 位的，那就没办法了。）

现在的 Meltdown 补丁中，强制将用户进程的虚拟内存空间与内核的虚拟内存区域完全分开。在这个修复方案中，内核并没有映射到每个进程的虚拟内存空间的顶部，并保持隐身，只在需要处理中断或系统调用时才出现。相反，内被转移到单独的虚拟地址空间和环境中。这个修复方案又称作“内核页面表隔离”（KPTI），可防止恶意软件利用“Meltdown”漏洞从用户模式读取内核内存。

在上下文之间来回切换（从用户进程上下文到内核上下文又返回到用户进程）需要重新加载页表、需要一个描述用进程的集合以及另一个描述内核。这些表将进程或内核的虚拟内存映射到 RAM 或交换空间的物理块中。这些上下从用户进程切换到内核进程不仅需要时间，而且还会刷新所有缓存的虚拟内存到物理内存的转换。这些最终会对性造成影响，在涉及大量 **IO** 或系统调用的工作负载时，影响更大。但是对于 **PCID** 而言，不需要在每个上下文切换刷新整个转换的后备缓冲区（**TLB**）缓存，因为选定的 **TLB** 条目可以保留在处理器中。

2017 年 11 月发布的 Linux 4.14 内核首次可以支持 PCID，因此默认情况下，并非每个 Linux 实例都可支持 PCID 虚拟机上更难实现。

企业 Java biz Azul Systems 的 CTO 兼首席技术官 Gil Tene 在周日发布的 Google Groups 博文中表示，PCID 已经成为特尔 x86 平台安全性和高性能的关键因素。但是他声明，在他看到的许多虚拟化的 Linux 实例中并不存在 PCID。

> 大多数 KVM 访客（基于内核的虚拟机）没有使用 PCID，而大多数 VMware 访客中都存在 PCID。此外，大约一半的 AWS 实例没有 PCID。如果没有 PCID，系统就会在不安全的环境中运行（默认情况下会关闭 Meltdown 自动修复），或者就是系统运行得太慢，导致用户甚至想干脆被入侵来摆脱太慢的痛苦。

总之，如果用户在打补丁后发现性能下降，可以查看自己的内核配置并启用 **PCID**。当然，如果你的芯片不具备 PC 功能，那就默默等待吧。

*参考来源：**TheRegister**，**Reuters**，**AngelaY** 编译整理，转载请注明来自 **FreeBuf.COM**

上一篇：
BUF早餐铺 | 微软修复56个安全问题；Reddit 用户比特币被盗；支付宝因年度账单事件被约谈；中国内地iCloud服务将
下一篇：旧版Windows打上CPU补丁后会出现性能下降

已有 5 条评论

f4ckbaidu (1级) 百毒一生黑 2018-01-11 1楼 回

对游戏性能几乎没影响，重度io性能影响严重

亮了

Sinohara (1级) 2018-01-11

@ f4ckbaidu 玩过足球经理不?

亮了

幕刃 2018-01-11 2楼 回

2017 年 11 月发布的 PCID 4.14内核首次支持 Linux

PCID内核？支持Linux？

难道不是Linux内核支持PCID？

亮了

中庸书生 2018-01-11 3楼 回

不是所有的补丁都是合适的

亮了

caish2007 (2级) 2018-01-12 4楼 回

继续观望。升级失败变砖，这风险很大。等补丁稳定了再升吧。

亮了

选择文件 未选择任何文件

昵称

请输入昵称

必须 您当前尚未登录。登陆? 注册

邮箱

请输入邮箱地址

必须（保密）

表情 插图

提交评论(Ctrl+Enter)

AngelaY
LIE TO ME

115
文章数

58
评论数

最近文章

- 芯片漏洞新进展：英特尔公布补丁对性能影响的测试结果；Meltdown的POC在Github上公开；NVIDIA更新GPU驱动以应对漏洞；IBM开始发放补丁；Ubuntu 16.04打补丁后出现boot问题
  2018.01.11
- 芯片漏洞不只是修复那么简单：补丁对性能的影响已经显现；部分企业选择暂缓修复
  2018.01.11
- BUF早餐铺 | 微软修复56个安全问题；Reddit 用户比特币被盗；支付宝因年度账单事件被约谈；中国内地iCloud服务将由国内公司负责
  2018.01.11

浏览更多

相关阅读

苹果确认Meltdown和Spectre漏洞影响…

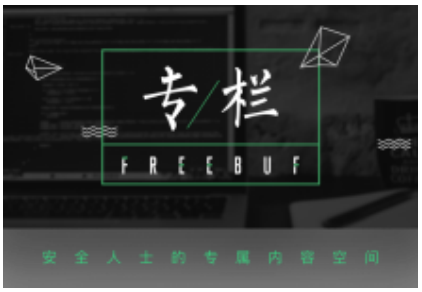
处理器A级漏洞Meltdown（熔毁）和S…

处理器安全漏洞Meltdown和Spectre爆…

旧版Windows打上CPU补丁后会出现性…

史上最大CPU漏洞Meltdown & Spectre …

特别推荐



关注我们 分享每日精选文章