CPU 芯片漏洞：Meltdown 与 Spectre 的问题与解决方案

V1.1

北京德源远大科技有限公司

2018 年 1 月 16 日

一、 综述：

该类型漏洞属于 CPU 设计逻辑缺陷，很难进行修复。

对云服务商家危害较大，对个人用户危害不大。

漏洞主要用于信息泄露，并不能对目标内存地址进行任意修改。

漏洞影响范围较大，但攻击难度大，截至目前，尚未发现相关攻击案例，仅停留在实验室理论攻击测试。

攻击者必须要有执行权限才能进行攻击，对于一般用户只要不被执行恶意代码（比如访问恶意网站），就不会被 Meltdown 与 Spectre 攻击。但是在云端，攻击者可以租赁虚拟机来执行攻击者想要执行的任意代码，从而获取宿主物理机以及其它租户的信息。

建议六代以上新机器可以升级 bios，其他机型仅升级操作系统补丁和升级浏览器。

二、 漏洞发现：

2018 年 1 月 3 日，Google Project Zero（GPZ）团队安全研究员 Jann Horn 在其团队博客中爆出 CPU 芯片的两组漏洞，分别是 Spectre（幽灵）和 Meltdown（熔断）。

下表是微软公司总结的漏洞明细：

Vuln. Name	CVE	Variant	Public Vuln. Name	Windows Changes	Silicon Microcode Update Required
Spectre	2017-5753	1	Bounds Check Bypass	Recompiled binaries in Windows Updates Edge, IE updated to prevent JavaScript exploit	No
Spectre	2017-5715	2	Branch Target Injection	Calling new CPU instructions to eliminate branch speculation in risky situations	Yes
Meltdown	2017-5754	3	Rogue Data Cache Load	Isolate kernel and user mode page tables	No

其中第一种形式（Variant 1，简称 V1）“Bounds Check Bypass（绕过边界检查/边界检查旁路）”和第二种形式“Branch Target Injection（分支目标注入）”属于 Spectre（幽灵），而第三种“Rogue Data Cache Load（恶意的数据缓存载入）”则属于 Meldown（熔断）。

这两组漏洞早在 2017 年 6 月就已经由 GPZ 团队向英特尔提交，并且英特尔在最新的处理器中进行了细微的改进。

三、 漏洞影响：

CPU：INTEL、AMD、ARM（高通、联发科、三星等平台）、IBM POWER CPU、NVIDIA GPU

操作系统：Windows、Linux、macOS、IOS、Android

虽然英特尔的 CPU 漏洞已经存在 20 年之久，影响面十分广泛，但是截至目前，尚未发现相关攻击案例。

因为发起攻击的难度比较大，“由于此漏洞是 CPU 硬件级别的，对这类漏洞的研究需要很深的专业知识，门槛比一般的软件应用漏洞挖掘要高很多。同时由于这两组漏洞只会造成信息泄露，不依靠其他漏洞很难发起完整的远程攻击。”

“侧信道攻击（英特尔将此次被利用漏洞的攻击称为测信道攻击 Side Channel attack）其实不是现在才有的，但 CPU 漏洞无疑提高了被攻击后的风险，使攻击者获得更多数据。但是这一切的前提是，之前一系列操作都没有被安全软件和系统安全机制甚至硬件安全机制察觉，这本身也是很难的。”

攻击案例尚未发生的另一方面原因在于，很多人未意识到芯片设计存在漏洞，或者不认为这是漏洞。

四、 漏洞原理及危害：

简单地说，漏洞会造成 CPU 运作机制上的信息泄露。在实际攻击场景中，攻击者在一定条件下可以达到如下恶意目的：

1.泄露出本地操作系统底层运作信息，秘钥信息等；

2.通过获取泄露的信息，可以绕过内核(Kernel)，虚拟机超级管理器(HyperVisor)的隔离防护；

3.云服务中，可以泄露到其它租户隐私信息；

4.通过浏览器泄露受害者的帐号，密码，内容，邮箱, cookie 等用户隐私信息；

比较可怕的是这个漏洞同样可以攻击到 RING 0 层面，也就是 Intel ME 这个级别的 CPU 厂商保留区，理论上可以完全控制这台电脑。

对于个人终端用户，利用 Meltdown 与 Spectre 漏洞，低权限用户可以访问内核的内容，泄露本地操作系统底层的信息、秘钥信息等，通过获取泄露的信息，可以绕过内核的隔离防护;如果配合其它漏洞，可以利用该漏洞泄露内核模块地址绕过 KASLR 等防护机制实现其他类型的攻击进行提权。另外，利用浏览器 JIT 特性预测执行特殊的 JIT 代码，从而读取整个浏览器内存中的数据，泄露用户帐号，密码，邮箱, cookie 等隐私信息。

对于云服务中的虚拟机 ,可以通过相关攻击机制获取完整的物理机的 CPU 缓存数据，绕过虚拟机超级管理器（Hypervisor）的隔离防护，以泄露其它租户隐私信息。

然而 Meltdown 与 Spectre 主要用于信息泄露 ,并不能对目标内存地址进行任意修改。攻击者必须要有执行权限才能进行攻击，对于一般用户只要不被执行恶意代码（比如访问恶意网站），就不会被 Meltdown 与 Spectre 攻击。但是在云端，攻击者可以租赁虚拟机来执行攻击者想要执行的任意代码，从而获取宿主物理机以及其它租户的信息。可见此次 CPU 漏洞对各云服务商冲击还是非常大的。各大云厂商也分别针对此次芯片漏洞发布应对公告。

总体来看，这次漏洞虽然影响广泛，但利用复杂，加上限制也很大，实施起来并不是那么容易。漏洞这个攻击方式需要被攻击的数据在攻击触发时刚好出现在内存、虚拟内存或 CPU 缓存中，病毒必须足够聪明，所以攻击难度比较大。

五、　　漏洞修复：

对于 V1，Windows 的解决方式是二进制编译器更新和从 JS 端加固浏览器。

对于 V2，微软需要 CPU 指令集更新，即更新 bios，屏蔽这部分用于提升性能的优化算法。

对于 V3，需要分离内核和用户层代码的页表。

具体来说就是：

1、打补丁。升级微软 1 月补丁，但目前该补丁存在兼容性问题，存在升级失败问题，对 amd 处理器平台，会造成蓝屏死机，目前微软正在商讨解决方案。

2、升级驱动。升级主板、显卡驱动程序。

3、升级 BIOS。升级主板 bios。

4、升级浏览器。微软 1 月补丁会升级 IE11 浏览器，使其具备免疫特性。其他浏览器也建议升级到最新版本。Chrome 用户，请在地址栏中，输入 chrome://flags/#enable-site-per-process，然后按 Enter 键，再点击“Strict site isolation”旁边的启用(如果系统没有显示“Strict site isolation”,请更新 Chrome)。最后点击立即重新启动。

Firefox 用户，请升级至 57.0.4 及以上版本。

六、 性能影响与厂家对策：

微软的测试：

如果不更新 BIOS，仅更新软件，则有少许性能影响。

如更新 bios，则对英特尔第六、七、八代处理器 Skylake/KabyLake/Coffee Lake 影响不大。对 1995 年至英特尔第六代处理器以前的 CPU 影响较大。具体如下：

1、搭载 Skylake / Kaby Lake 或者更新的处理器平台（六、七、八代）的 Windows 10 系统，降幅在个位数，意味着，绝大多数用户都感受不到变化，因为即便慢，也是在毫秒之内。

2、搭载 Haswell（四代）或者更早的处理器的 Windows 10 平台，影响已经有些显著了，可能部分用户已经可以觉察出来。

3、搭载 Haswell 或者更早的处理器的 Windows 7 / 8．1 平台，大部分用户会明显感受到性能削弱。

4、任何处理器的 Windows Server 平台，尤其是密集 I / O 环境下，在执行代码分离操作时性能降幅会异常明显。

微软称，Windows 7 / 8 在架构时由于使用了过多的用户到内核过渡，导致影响更明显。

硬盘 4K 读写性能降低较多，固态硬盘更甚。

微软对策：提供操作系统和浏览器的修复补丁。微软很快发布了补丁 KB4056892，但有些用户表示安全更新版本导致 AMD Athlon 驱动的计算机崩溃。后来微软确认补丁存在兼容性问题，现已紧急撤回。目前，微软已经停止了 9 个补丁向 AMD 平台的分发工作(主要是 Win10 的 KB4056892 和 Win7 的 KB4056894)，正和 AMD 一道联手解决。

LINUX：提供操作系统更新。

INTEL：配合提供操作系统修复补丁、硬件驱动

AMD：CPU 架构对 V3 是完全免疫，但 v1 则需要配合操作系统更新实现。

ARM：请升级苹果、安卓手机系统到最新。

NVIDIA：提供驱动更新 390.65，正在测试 v2 的影响。

IBM：提供 BIOS 更新和操作系统更新

苹果：1 月 9 日，苹果发布 Spectre 漏洞修复补丁，主要包括 macOS High Sierra 10.13.2 版本，iOS 11.2.2 版本和 Safari 11.0.2 版本，针对的设备是智能手机、平板电脑和台式电脑。

七、 维护建议：

建议六代以上新机器可以升级 bios，其他机型仅升级操作系统补丁和升级浏览器。可根据文章第五点所列出项目进行修复。注意 amd 处理器的计算机暂时不要安装最新补丁，以免出现蓝屏无法进入系统。

建议使用 360CPU 漏洞免疫工具，该工具可一键检测电脑是否存在漏洞，全方位排查补丁兼容性，并为受到漏洞影响的系统及浏览器推送安全更新，有效免疫 CPU 漏洞。针对没有补丁的系统，开启 360 安全卫士能够全面防御攻击，把漏洞风险降到最低。

下载地址：http://down.360safe.com/cpuleak_scan.exe