# 处理器 Meltdown/Spectre 漏洞修复简要指南

| |
|---|
| 安全报告：处理器 Meltdown/Spectre 漏洞修复简要指南 |
| 报告编号：B6-2018-010401 |
| 报告来源：360CERT |
| 报告作者：360 安全团队 |
| 版本：版本 2 |
| 保密范围：公开 |
| 更新日期：2017 年 1 月 9 日 |

# 目 录

0x00 概述 ..... 3

0x01 漏洞影响面 ..... 3

影响面 ..... 3
漏洞编号 ..... 3

0x02 部分漏洞信息 ..... 4

0x03 安全建议 ..... 5

Intel 的缓解建议 ..... 6
PC 终端用户 ..... 6
IDC/云系统管理员 ..... 8
云平台租户 ..... 11

0x04 FAQ 常见问题 ..... 11

0x05 时间线 ..... 12

0x06 相关厂商公告 ..... 12

# 0x00 概述

2018 年 1 月 4 日，Jann Horn 等安全研究者披露了"Meltdown"(CVE-2017-5754)和"Spectre"(CVE-2017-5753 & CVE-2017-5715)两组 CPU 特性漏洞。

据悉，漏洞会造成 CPU 运作机制上的信息泄露，低权级的攻击者可以通过漏洞来远程泄露用户信息或本地泄露更高权级的内存信息。

实际攻击场景中，攻击者在一定条件下可以做到，

- 泄露出本地操作系统底层运作信息，秘钥信息等；
- 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；
- 云服务中，可能可以泄露到其它租户隐私信息；
- 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；

目前相关的平台，厂商，软件提供商都在积极应对该系列漏洞，部分厂商提供了解决方案。

经过 360 安全团队评估，"Meltdown"和"Spectre"漏洞影响重要，**修复流程较复杂，建议相关企业/用户在充分了解补丁风险的基础上，作好相关的修复评估工作。**

# 0x01 漏洞影响面

## 影响面

漏洞风险等级重要，影响广泛：

- 近 20 年的 Intel，AMD，Qualcomm 厂家和其它 ARM 的处理器受到影响；
- 因为此次 CPU 漏洞的特殊性，包括 Linux，Windows，OSX，iOS，Android 等在内的操作系统平台参与了修复；
- 360 安全浏览器，Firefox，Chrome，Edge 等浏览器也发布了相关的安全公告和缓解方案；

## 漏洞编号

- Meltdown：CVE-2017-5754
- Spectre ：CVE-2017-5715 和 CVE-2017-5753

# 0x02 部分漏洞信息

注： 本段文字中直接引用了相关安全公告，如有异议请联系 cert@360.cn。

现代处理器（CPU）的运作机制中存在两个用于加速执行的特性，推测执行（Speculative Execution）和间接分支预测（Indirect Branch Prediction)。

表面上看，处理器是依次顺序执行既定的处理器指令。但是，现代处理器为了更好利用处理器资源，已经开始启用并行执行，这个技术已经应用了 20 年左右(1995 年开始)。假设，基于猜测或概率的角度，在当前的指令或分支还未执行完成前就开始执行可能会被执行的指令或分支，会发生什么？如果猜对了，直接使用，CPU 执行加速了。如果猜测不正确，则取消操作并恢复到原来的现场（寄存器，内存等），结果会被忽略。整个过程并不会比没有猜测的时候慢，即 CPU 的推测执行（Speculative Execution）技术。

不幸的是，尽管架构状态被回滚了，仍然有些副作用，比如 TLB 或缓存状态并没有被回滚。这些副作用随后可以被黑客通过旁道攻击(Side Channel Attack)的方式获取到缓存的内容。如果攻击者能触发推测执行去访问指定的敏感数据区域的话，就可能可以读取到更高特权级的敏感数据。

此外，猜测过程是可以被“污染”的，攻击者可以构造出类似 ROP 攻击的逻辑去影响推测过程。根据作者提供的思路，主要有三种场景：

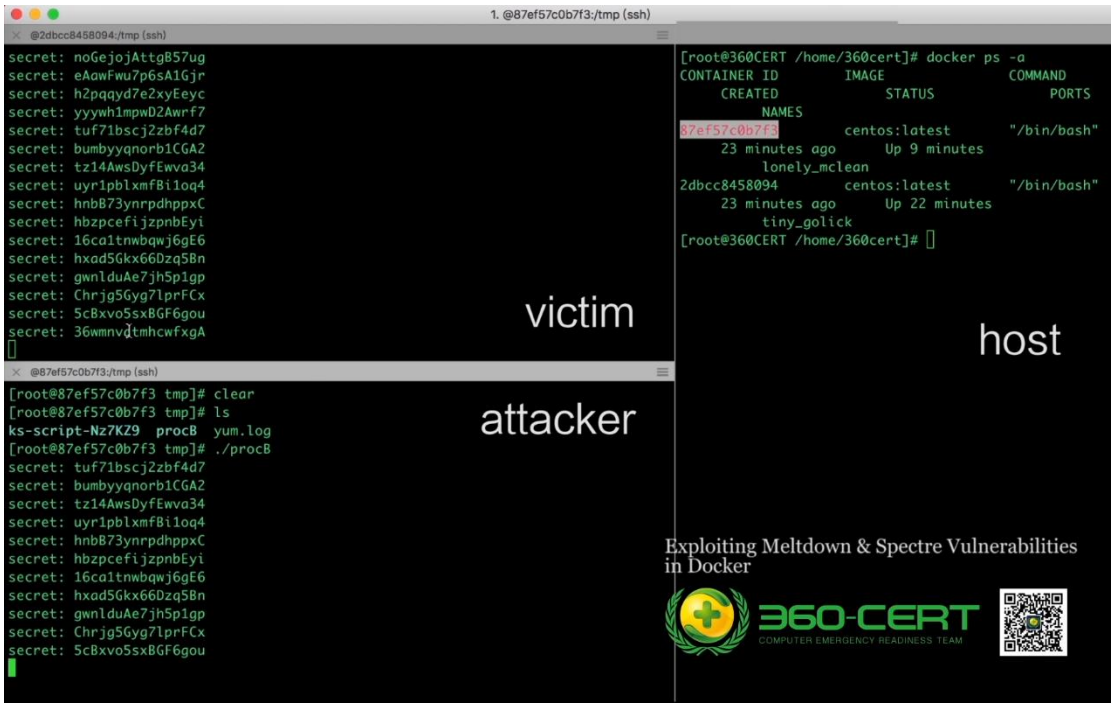
1. “边界检查绕过”：通过污染分支预测，来绕过 kernel 或 hypervisor 的内存对象边界检测。比如，攻击者可以对高权级的代码段，或虚拟环境中 hypercall，通过构造的恶意代码来触发有越界的数据下标，造成越界访问。
2. “分支目标注入”： 污染分支预测。抽象模型比较好的代码往往带有间接函数指针调用的情况，CPU 在处理时需要会进行必要的内存访问，这个过程有点慢，所以 CPU 会预测分支。攻击者可以通过类似的 ROP 的方式来进行信息泄露。
3. “流氓数据加载”：部分 CPU 上，为了速度并不是每次都对指令作权限检查的，检查的条件存在一定的缺陷；

实际攻击场景中，攻击者在一定条件下可以做到，

- 泄露出本地操作系统底层运作信息，秘钥信息等;
- 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;
- 云服务中，可以泄露到其它租户隐私信息；
- 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；

360CERT 和 360GearTeam 对漏洞进行了研究性质的尝试。在 Linux+Docker 的环境下进行的攻击演示，通过利用 Meltdown 或 Spectre 漏洞，模拟在独立的 Docker 容器 A 对同一个宿主中的 Docker 容器 B 进行敏感数据（密码）窃取的尝试。

声明：本试验是 360CERT 针对 CPU 的 Meltdown 和 Spectre 漏洞作的一个研究性测试，实际的 Docker 攻击利用场景中需要满足特殊和较严苛的限制条件。




目前几大系统厂商各自在操作系统内核中引入了 KPTI 的技术，旨在和用户态的页表隔离，解决"Meltdown"漏洞问题。但根据相关测试信息显示，修复补丁可能带来 5%到 30%性能上的损失，其中个人终端用户基本感觉不到，部分服务器的 IO 场景可能造成较大的性能损耗。

针对"Spectre"漏洞，相关操作系统厂商和芯片厂商积极配合，通过微码固件更新和操作系统更新的方式进行解决。

# 0x03 安全建议

**360CERT 建议企业/用户务必在充分了解相关风险的基础上，作好相关修复评估工作：**

1. "Meltdown"和"Spectre"漏洞修复流程相对复杂，部分平台上暂时没有统一的修复工具；
2. 芯片厂商（如：Intel）的微码固件补丁需要通过所在硬件 OEM 厂商获取（如：Dell，联想等）；
3. 可能会有部分软件不兼容问题（如 Windows 平台下的部分杀毒软件等）；
4. 在云平台或特定应用场景中可能造成较大幅度的性能损失，升级前请充分了解相关信息；

具体评估和修复工作，可以参考以下建议和相关厂商的安全公告：

# Intel 的缓解建议

Intel 已经和产业界联合，包括其它处理器厂商和软件厂商开发者，来缓解之前提到的三种攻击类型。缓解策略主要聚焦在适配市面产品和部分在研产品。缓解除了解决漏洞本身之外，还需要兼顾到性能影响，实施复杂度等方面。

启用处理器已有的安全特性（如 Supervisor-Mode Execution Protection 和 Execute Disable Bit ）可以有效提高攻击门槛。相关信息可以参阅 Intel 的相关资料。

Intel 一直在与操作系统厂商，虚拟化厂商，其它相关软件开发者进行合作，协同缓解这些攻击。作为我们的常规研发流程，Intel 会积极保证处理器的性能。

来源：
*https://newsroom.intel.com/wp-content/uploads/sites/11/2018/01/Intel-Analysis-of-Speculative-Execution-Side-Channels.pdf*

# PC 终端用户

PC 终端用户，建议用户根据各个平台进行如下对应操作：

**微软 Windows**

修复步骤如下：

1. 更新对应的浏览器，缓解"Spectre"漏洞攻击；

| 浏览器 | 缓解措施 |
| --- | --- |
| 360 安全浏览器 | 升级 360 安全浏览器到 9.1 及以上版本 |
| Firefox | 升级 Firefox 到 57.0.4 及以上版本 |
| Chrome | 1. 在地址栏中，输入 chrome://flags/#enable-site-per-process，然后按 Enter 键。<br>2. 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。)。<br>3. 点击立即重新启动 |

| | |
|---|---|
| Edge/IE | 补丁集成于 Windows 补丁中，请参考“更新 Windows 补丁” |

2. 更新芯片厂商的微码补丁

| 芯片厂商 | 微码补丁 |
|---|---|
| Intel | 微码补丁发布流程较复杂，请关注并通过 Intel 的相关硬件 OEM 提供商渠道更新（如戴尔,联想，惠普等）。 |

如：

Dell XPS 15 9560 System BIOS

This package provides the Dell System BIOS update and is supported on Dell XPS 15 9560 for Windows Operating Systems.

补丁和增强功能

Update to the latest CPU microcode to address CVE-2017-5715

版本 版本1.7.0、1.7.0

类别 BIOS

发布日期 29 十二月 2017

上次更新 08 一月 2018

重要性 紧急

可用格式

文件格式： Windows/DOS
文件名： XPS_15_9560_1.7.0.exe
下载类型： HTTP
文件大小： 10 MB
格式说明: 此文件格式包含BIOS可执行文件。可以使用通用格式(Windows/MS DOS)，从任何Windows或MS DOS环境安装

下载文件 添加到下载列表中

3. 更新 Windows 补丁

用户可直接下载 360 安全卫士 CPU 漏洞免疫工具进行更新：

http://down.360safe.com/cpuleak_scan.exe

**注意：根据微软提供的信息，依然存在部分不兼容（如杀毒软件，部分 AMD 的 CPU）的风险，请充分了解风险后再选择是否更新：**

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

**苹果 OSX**

苹果在 Mac OSX High Sierra 10.13.2 及更高版本修复了 Meltdown 和 Spectre 漏洞，请直接升级。

**Android & iOS**

苹果在 iOS 11.2.2 及更高版本修复了 Spectre 漏洞；

Android 产品将于近期更新，尽请留意。

# IDC/云系统管理员

---

目前部分 IDC/云基础架构厂商已经提供了初步解决方案，但是由于补丁带来的风险和性能损耗暂时没有明确，权威的结论。

**请系统管理员尽量做到：**

1. 积极联系相关的上游了解相关的风险和解决方案，协同制定解决方案；
2. 需要重点关注补丁带来风险和性能损耗评估；
3. 从宏观和微观层面，制定完善，可行的修复和测试流程方案；
4. 涉及到的微码固件补丁请联系硬件 OEM 厂商，协同修复，测试，评估；

以下是相关厂商提供的解决方案：

Linux-Redhat/CentOS 发行版

Redhat 提供了一份产品的修复状态清单，建议用户参照该清单进行更新。具体用户可以参考：

- https://access.redhat.com/security/vulnerabilities/speculativeexecution
- https://access.redhat.com/articles/3311301#page-table-isolation-pti-6

鉴于更新完补丁后，在部分应用场景下会造成性能下降，RedHat 方面提供了运行时的解决方案：

- https://access.redhat.com/articles/3311301#page-table-isolation-pti-6

用户可以通过以下命令临时关闭或部分 KPTI，Indirect Branch Restricted Speculation (ibrs)，Indirect Branch Prediction Barriers (ibpb) 等安全特性。

```
# echo 0 > /sys/kernel/debug/x86/pti_enabled
# echo 0 > /sys/kernel/debug/x86/ibpb_enabled
# echo 0 > /sys/kernel/debug/x86/ibrs_enabled
```

该特性需要使用 debugfs 文件系统被挂在，RHEL 7 默认开启了。 在 RHEL 6 中可以通过以下命令开启：

```
# mount -t debugfs nodev /sys/kernel/debug
```

用户可以通过以下命令查看当前安全特性的开启状态：

```
# cat /sys/kernel/debug/x86/pti_enabled
# cat /sys/kernel/debug/x86/ibpb_enabled
# cat /sys/kernel/debug/x86/ibrs_enabled
```

Intel 芯片在修复后默认如下：

```
pti 1 ibrs 1 ibpb 1 -> fix variant#1 #2 #3
pti 1 ibrs 0 ibpb 0 -> fix variant#1 #3 (for older Intel systems with no microcode update available)
```

AMD 芯片在修复后默认如下：

```
pti 0 ibrs 0 ibpb 2 -> fix variant #1 #2 if the microcode update is applied
pti 0 ibrs 2 ibpb 1 -> fix variant #1 #2 on older processors that can disable indirect branch prediction without microcode updates
```

在没有微码固件补丁升级的情况下：

```
# cat /sys/kernel/debug/x86/pti_enabled
1
# cat /sys/kernel/debug/x86/ibpb_enabled
0
# cat /sys/kernel/debug/x86/ibrs_enabled
0
```

注：Redhat 等厂商并不直接提供芯片厂商的微码，需要用户到相关的硬件 OEM 厂商进行咨询获取。

**Linux-Ubuntu 发行版**

目前 Ubuntu 只完成对 Meltdown(CVE-2017-5754)漏洞在 x86_64 平台上的更新。

请关注 Ubuntu 的更新链接：

*https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SpectreAndMeltdown*

Linux-Debian 发行版

目前 Debian 完成了 Meltdown(CVE-2017-5754)漏洞的修复。

关于 CVE-2017-5715 和 CVE-2017-5753 请关注 Debian 的更新链接：

https://security-tracker.debian.org/tracker/CVE-2017-5753
https://security-tracker.debian.org/tracker/CVE-2017-5715

**微软 Windows Server**

建议用户开启系统自动更新功能，进行补丁补丁安装。

**根据微软提供的信息，依然存在部分不兼容（如杀毒软件，部分 AMD 的 CPU）的风险，请充分了解风险后再选择是否更新。**

更多信息请查看：

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

**Xen 虚拟化**

目前 Xen 团队针对 Meltdown，Spectre 漏洞的修复工作依然在进行中，请关注 Xen 的更新链接：

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

**目前 Xen 暂时没有性能损耗方面的明确评估，请谨慎更新。**

**QEMU-KVM 虚拟化**

QEMU 官方建议通过更新 guest 和 host 操作系统的补丁来修复 Meltdown 漏洞，并表示 Meltdown 漏洞不会造成 guest 到 host 的信息窃取。

针对 Spectre 的变种 CVE-2017-5715，QEMU 方面正在等待 KVM 更新后再修复，目前 KVM 在进行相关补丁整合。**需要注意的是，热迁移不能解决 CVE-2017-5715 漏洞，KVM 需要把 cpu 的新特性 expose 到 guest 内核使用，所以 guest 需要重启。**

相关信息请查阅：

https://www.qemu.org/2018/01/04/spectre/
https://marc.info/?l=kvm&m=151543506500957&w=2

## 云平台租户

360CERT 建议云平台用户，

1. 关注所在云厂商的安全公告，配合相关云厂商做好漏洞补丁修复工作；
2. 充分了解和注意补丁带来的风险和性能损耗方面的指标；
3. 更新前可以考虑使用相关快照或备份功能；

# 0x04 FAQ 常见问题

1. 问题： Meltdown 和 Spectre 漏洞具体技术影响。 比如利用这两个漏洞发动攻击是否容易，什么条件下触发，危害多大？

回答： Meltdown 和 Spectre 漏洞在一定的条件下都可以触发，例如通过本地环境,浏览器环境， Xen/QEMU-KVM 中恶意租户 Guset 的场景来触发和攻击，虽然目前尚未发现公开的攻击代码，但能够对用户造成帐号， 密码， 内容， 邮箱, cookie 等隐私信息泄露潜在危害。从以往情况看，在漏洞暴露后一定时间内，就可能出现可利用的攻击代码。对此，我们需要保持高度警惕。

Meltdown 漏洞主要作用于本地环境，可用于越权读内核内存。Spectre 由于不会触发 trap，可以用于浏览器攻击，以及虚拟机 guest/host 攻击，及其它存在代码注入（如即时编译 JIT）程序的潜在攻击。具体技术情况需如下：

| 类型 | 利用难度 | 本地环境触发 | 浏览器触发 | 内核数据泄露 | 虚拟化Guest内核攻击 | 虚拟化Host/HyperVisor攻击 | 其它JIT程序潜在攻击 |
|---|---|---|---|---|---|---|---|
| Meltdown | 较难 | 是 | 否 | 是 | 是 | 部分场景可用 | 否 |
| Spectre | 较难 | 是 | 是 | 是 | 是 | 部分场景可用 | 是 |

2. 问题：当前对漏洞的处置情况到底怎么样了，业界解决情况如何，有没有比较完善的解决方案。目前能解决到什么程度，怎么才能彻底解决？

回答：目前大部分的个人终端操作系统（如 Windows, MacOS, iOS, Android）都可以通过直接的渠道进行更新解决，其中 Windows 平台存在部分杀毒软件不兼容风险。针对 IDC 或云厂商相关的系统管理员，除了还需要再继续评估补丁的兼容性风险外，更需要再进一步评估补丁可能带来的较大幅度的性能损耗，目前芯片厂商也在积极和大型 IDC，云服务提供商协同制定更完善的解决方案。

360CERT 建议该怎么解决，后续该怎么做？

回答：360CERT 建议，一方面，PC/手机的个人用户可以直接通过操作系统厂商或第三方安全厂商提供的补丁来解决。另一方面，针对补丁给企业带来修复难题，大型 IDC/企业/云

厂商，芯片厂商，操作系统厂商，信息安全公司要协同起来，在补丁方案，补丁风险评估，补丁导致的性能损耗评估，综合补丁标准方案，一体化补丁等方面形成合力，在保证业务稳定的情况下逐步或分阶段推进补丁的修复工作。

## 0x05 时间线

2018-01-04 Google 的 Jann Horn 发布漏洞信息

2018-01-04 360 安全团队发布预警通告

2018-01-09 360 安全团队发布简要修复指南

## 0x06 相关厂商公告

- Intel
  https://newsroom.intel.com/news/intel-responds-to-security-research-findings/
  https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr
  https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html
  https://newsroom.intel.com/wp-content/uploads/sites/11/2018/01/Intel-Analysis-of-Speculative-Execution-Side-Channels.pdf
- Microsoft
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002
  https://support.microsoft.com/en-us/help/4073119/windows-client-guidance-for-it-pros-to-protect-against-speculative-exe
- 联想
  https://support.lenovo.com/us/zh/solutions/len-18282
- 华为
  http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180106-01-cpu-en
- Amazon
  https://aws.amazon.com/de/security/security-bulletins/AWS-2018-013/
- ARM
  https://developer.arm.com/support/security-update
- Google
  https://googleprojectzero.blogspot.co.at/2018/01/reading-privileged-memory-with-side.html
  https://www.chromium.org/Home/chromium-security/ssca

https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html

- MITRE

  http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715

  http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5753

  http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5754

- Red Hat

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

  https://access.redhat.com/articles/3311301#page-table-isolation-pti-6

- Apple

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

- Xen

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

- Mozilla

  https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/

- VMware

  https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html

- AMD

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

- SuSe

  https://www.suse.com/support/kb/doc/?id=7022512

- Ubuntu

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

- QEMU-KVM

  https://marc.info/?l=kvm&m=151543506500957&w=2

  https://www.qemu.org/2018/01/04/spectre/

- 漏洞报告

  https://meltdownattack.com/meltdown.pdf

  https://spectreattack.com/spectre.pdf

  https://googleprojectzero.blogspot.co.uk/2018/01/reading-privileged-memory-with-side.html

- 360

  http://down.360safe.com/cpuleak_scan.exe