预警编号：YJ-2018001

# 恒安嘉新

# 关于 CPU 处理器内核

# 存在 Meltdown 和 Spectre 漏洞

# 安全预警通告


**恒安嘉新（北京）科技股份公司**

**2018 年 1 月 05 日**

# 1 漏洞描述

近期,互联网爆出 CPU 处理器内核的 Meltdown 漏洞( CVE-2017-5754 ）和 Spectre 漏洞（ CVE-2017-5715 和 CVE-2017-5753 ）。利用上述漏洞，攻击者可以绕过内存访问的安全隔离机制,使用恶意程序来获取操作系统和其他程序的被保护数据，造成内存敏感信息泄露。该漏洞危害程度为高危(High)。

# 2 影响范围

该漏洞存在于英特尔（ Intel ）x86-64 的硬件中，在 1995 年以后生产的 Intel 处理器芯片都可能受到影响。同时 AMD、Qualcomm、ARM 处理器也受到影响。

同时使用上述处理器芯片的操作系统（ Windows、Linux、Mac OS、Android ）和云计算平台也受此漏洞影响

# 3 漏洞原理

现代的计算机处理器芯片通常使用“推测执行”（ speculative execution ）和“分支预测”（ Indirect Branch Prediction ）技术实现对处理器计算资源的最大化利用。但由于这两种技术在实现上存在安全缺陷，无法通过正确判断将低权限的应用程序访存与内核高权限的访问分开,使得攻击者可以绕过内存访问的安全隔离边界，在内核中读取操作系统和其他程序的内存数据，造成敏感信息泄露。具体如下：

1）Meltdown 漏洞的利用破坏了用户程序和操作系统之间的基本隔离，允许攻击者未授权访问其他程序和操作系统的内存，获取其他程序和操作系统的敏感信息。

2）Spectre 漏洞的利用破坏了不同应用程序之间的安全隔离，允许攻击者借助于无错程序（error-free）来获取敏感信息。

# 4 修复建议

目前，操作系统厂商已经发布补丁更新，如 Linux，Apple 和 Android，微软也已发布补丁更新。强烈建议用户及时下载补丁进行更新，参考链接：

Linux：http://appleinsider.com/articles/18/01/03/apple-has-already-partially-implemented-fix-in-macos-for-kpti-intel-cpu-security-flaw

Android：https://source.android.com/security/bulletin/2018-01-01

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

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

Intel：https://newsroom.intel.com/news/intel-responds-to-security-research-findings/

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

Nvidia：https://forums.geforce.com/default/topic/1033210/nvidias-response-to-speculative-side-channels-cve-2017-5753-cve-2017-5715-and-cve-2017-5754/

Xen：https://xenbits.xen.org/xsa/advisory-254.html