TC260-PG-20181A

网络安全实践指南

—CPU 熔断和幽灵漏洞防范指引

全国信息安全标准化技术委员会秘书处

2018 年 1 月 16 日

本文档可从以下网址获得：
http://www.tc260.org.cn/front/postDetail.html?id=20180116090719

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全实践指南》（以下简称“实践指南”）是全国信息安全标准化技术委员会（以下简称“信安标委”，TC260）发布的技术文件。实践指南旨在推广网络安全标准，应对网络安全事件，改善网络安全状况，提高网络安全意识。

本实践指南是在分析总结相关厂商针对 CPU 熔断和幽灵漏洞发布的安全公告和漏洞补丁的基础上，通过研究提炼形成的，可为漏洞防范提供指引。

声　明

技术支持单位

本实践指南得到中标软件、360、华为技术、龙芯中科、华芯通、阿里云、百度云、腾讯、普华软件、中科曙光、成都海光、神州网信、天津麒麟、安恒等单位的技术支持。

摘　要

本实践指南分析总结了CPU、操作系统和云服务提供商等厂商针对熔断（Meltdown）和幽灵（Spectre）漏洞提供的缓解措施，给出了漏洞防范指引，并提供了部分厂商的官方安全公告和补丁链接。建议用户参考本实践指南给出的漏洞防范指引，及时采取安全措施应对安全威胁。

关键词：网络安全；熔断漏洞；幽灵漏洞；防范指引

一、漏洞描述

本实践指南应对的两个CPU漏洞分别为熔断（Meltdown，CNVD-2018-00303，对应CVE-2017-5754）和幽灵漏洞（Spectre，CNVD-2018-00302和CNVD-2018-00304，分别对应CVE-2017-5715和CVE-2017-5753）。熔断漏洞利用CPU乱序执行技术的设计缺陷，破坏了内存隔离机制，使恶意程序可越权访问操作系统内存数据，造成敏感信息泄露。幽灵漏洞利用了CPU推测执行技术的设计缺陷，破坏了不同应用程序间的逻辑隔离，使恶意应用程序可能获取其它应用程序的私有数据，造成敏感信息泄露。

熔断漏洞涉及几乎所有的Intel CPU和部分ARM CPU；幽灵漏洞涉及所有的Intel CPU、AMD CPU，以及部分ARM CPU。

由于上述漏洞来源于硬件，需要从CPU架构和指令执行机理层面进行修复。上述漏洞只能读取数据，不能修改数据，远程利用难度较大，尚未监测到利用上述漏洞的真实攻击案例。

二、风险分析

1. 漏洞风险分析

云服务提供商、服务器用户、云租户和个人用户均可能受到熔断和幽灵漏洞的威胁。其中云平台和部署在互联网环境下的服务器受攻击的风险更大。

（1）云服务提供商。云服务提供商包括公有云和私有云服务提供商。在云环境中，攻击者以云租户身份，可利用熔断或幽灵漏洞，绕过虚拟化平台内存隔离机制，直接访问虚拟化平台的内存，窃取平台敏感信息（如口令、密钥等），进一步获得管理员权限，可实现对整个云平台的控制。

（2）服务器用户。攻击者可利用熔断或幽灵漏洞，绕过服务器操作系统提供的安全隔离机制，直接访问服务器操作系统的内核空间，窃取内核敏感信息（如口令、密钥等），进一步获得管理员权限，可实现对整个服务器的控制。

（3）云租户。攻击者以云租户身份，可利用幽灵漏洞攻击云平台，绕过云平台提供的内存隔离机制，越权访问其他租户私有数据，可能导致其他租户敏感信息泄漏。

（4）个人用户。攻击者通过恶意脚本（如恶意JavaScript）攻击用户浏览器，可读取个人用户的浏览器数据，导致用户账号、密码、邮箱、cookie等信息泄漏。该恶意脚本可能是个人用户通过浏览器访问恶意网站时，下载到本地执行并感染的。

目前，熔断和幽灵漏洞的利用代码已披露，但尚未监测到利用这两类漏洞的真实攻击案例。主流厂商已开始积极应对，纷纷推出漏洞补丁，主流云服务提供商也已经评估风险，并按计划进行升级。

2. 升级风险分析

熔断漏洞和幽灵漏洞的补丁升级过程可能需要重启系统，会影响到用户业务的连续性。当前厂商提供的漏洞补丁普遍存在导致系统性能下降或影响稳定性等问题。

针对熔断和幽灵漏洞的 3 个变种，其补丁升级过程存在一定风险：

（1）变种 1（CVE-2017-5753，绕过边界检查型漏洞）的补丁升级需要更新操作系统，会影响业务的连续性，但对性能影响可以忽略不计。其中，云服务提供商可通过热迁移技术实现补丁升级，不需重启操作系统。

（2）变种 2（CVE-2017-5715，分支预测注入型漏洞）的补丁升级需要更新固件和操作系统，会影响业务连续性，性能影响较小。其中，云服务提供商可通过热迁移技术实现补丁升级，不需重启操作系统。

（3）变种 3（CVE-2017-5754，乱序执行的 CPU 缓存污染型漏洞）的补丁升级需要重启操作系统，会影响业务连续性，对 I/O 密集型业务系统的性能影响较大，对计算密集型业务系统的性能影响较小。

用户应充分评估漏洞补丁升级风险对业务的影响，重点关注补丁升级会造成的业务连续性中断和性能下降等风险。

三、漏洞防范指引

本实践指南主要为云服务提供商、服务器用户、云租户

和个人用户提供漏洞防范指引，以帮助用户防范熔断和幽灵漏洞，控制漏洞补丁升级所带来的负面影响。政府门户网站和政务信息系统，以及金融、能源、交通等行业信息系统，可根据其业务部署模式制定相应的升级方案。关于本实践指南中涉及的部分厂商官方补丁，请参见附录 A。升级完成后，建议用户对业务进行持续监控和性能评估，当发现升级失败、升级后业务不稳定、性能急剧下降等问题时，恢复系统到补丁升级前状态。

1. 云服务提供商

云服务提供商对云平台的补丁升级主要包括固件升级和云平台软件升级两部分。云服务提供商应在升级前联系云平台软硬件供应商，协同制定补丁升级方案，并密切关注相关开源社区安全公告。

（1）升级准备。应制定完整的云平台升级和测试验证方案，进行充分的测试，分析性能损耗、稳定性等情况，评估相关安全风险。应发布正式升级公告，告知云租户关于平台升级的具体时间点、升级可能带来的业务中断等风险，并为云租户自身应负责的补丁升级工作提供有效指导。

（2）升级实施。包括固件和云平台软件补丁升级。在升级前采用热迁移技术将云租户业务迁移到备用服务器。

——固件升级：目前主流 CPU 厂商提供了部分 CPU 的固件补丁，升级时需要寻求设备厂商足够技术支持，确认固

件补丁版本，从设备厂商官方网站下载相应补丁，实施升级。

——云平台软件升级：对于使用商业虚拟化产品的云平台，建议在平台软件供应商（如 VMWare、Xen Server、Hyper-V 等）的指导下完成升级工作。对于使用开源虚拟化技术实现的云平台，应关注对应的开源社区（如 Xen 和 Qemu-KVM），及时获取最新的补丁源码及升级指南。在综合考虑补丁风险、性能损耗因素后，参考产业优秀实践，确定可行的升级技术，明确升级流程，充分结合自身特点制定系统升级及失败恢复方案，有序开展升级工作。

2. 服务器用户

服务器用户升级主要包括固件、操作系统（含虚拟化平台）升级等工作。

（1）升级准备。制定漏洞升级方案，做好系统和数据备份，制定升级失败恢复方案，明确业务影响较小的补丁升级时间窗口。应寻求厂商技术支持，根据服务器硬件类型，评估是否需要升级固件。

（2）升级实施。包括固件升级、操作系统及虚拟化平台升级。升级前应安全关闭上层业务系统。

——固件升级：目前主流 CPU 厂商提供了部分 CPU 的固件补丁，应确认固件补丁版本，从设备厂商官方网站下载相应补丁，实施升级。

——操作系统及虚拟化平台升级：应根据服务器操作系

统（包括 Windows Server 系列、Linux 系列、UNIX 系列等）和虚拟化产品类型（包括 VMWare vSphere、Citrix XenServer 等），下载相应补丁并实施升级。

3. 云租户

云租户升级主要包括租户操作系统和应用升级等。

（1）升级准备。关注云服务提供商的安全公告，研究云服务提供商发布的升级指导。结合自身业务，确定受影响的操作系统和相关应用，评估性能、兼容性、业务连续性等方面的影响，制定升级计划和方案。执行升级前应备份相关数据和系统。

（2）升级实施。根据制定的升级方案，升级客户操作系统和上层应用。

4. 个人用户

尽管上述漏洞影响极为广泛，但漏洞利用条件较为苛刻，攻击成功率低。建议关注各操作系统厂商、浏览器厂商、整机厂商等的安全公告，采用系统自带的系统升级工具或第三方提供的漏洞管理工具下载和安装补丁，从而避免漏洞的影响。同时，个人用户应安装并及时更新防病毒软件，并养成良好上网习惯，不轻易浏览不信任的网站，不轻易点击来源不明的网页链接，提高安全防范意识。

附件 A: 部分厂商安全公告和补丁链接

类别	名称	官方链接
处理器	Intel	https://security-center.intel.com/ https://newsroom.intel.cn/press-kits/security-exploits-intel-products/
	AMD	http://www.amd.com/en/corporate/speculative-execution
	ARM	https://developer.arm.com/support/security-update
	IBM	http://www-01.ibm.com/support/docview.wss?uid=swg22012320 http://download.boulder.ibm.com/ibmdl/pub/software/server/firmware/SC-Firmware-Hist.html
	NVIDIA	http://nvidia.custhelp.com/app/answers/detail/a_id/4611
操作系统	微软	https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/ADV180002 https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in
	苹果	https://support.apple.com/zh-cn/HT208394

	Android	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
	RedHat	https://access.redhat.com/security/vulnerabilities/speculativeexecution https://access.redhat.com/articles/3311301#page-table-isolation-pti-6
	Ubuntu	https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SpectreAndMeltdown
	SUSE	https://www.suse.com/support/kb/doc/?id=7022512
	中标麒麟	安全公告： http://www.cs2c.com.cn/news/index.php?id=1120 产品补丁： http://ssms.cs2c.com.cn/otrs/pc?Action=PublicFAQExplorer;CategoryID=41
	普华	安全公告： http://www.i-soft.com.cn/type/4/3704.jhtml

		http://www.i-soft.com.cn/article/102461.jhtml 产品补丁： http://www.i-soft.com.cn/article/102461.jhtml
浏览器	Microsoft IE/Edge	https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/ADV180002
	Firefox	https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/
	Chrome	https://www.chromium.org/Home/chromium-security/ssca
	Safari	https://support.apple.com/zh-cn/HT208394
服务器	华为	http://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20180106-01-cpu-cn
	思科	https://blogs.cisco.com/security/talos/meltdown-and-spectre
	联想	https://support.lenovo.com/us/zh/solutions/len-18282
云服务	阿里云	安全公告： https://help.aliyun.com/noticelist/articleid/20700730.html

		帮助文档： https://help.aliyun.com/knowledge_detail/64951.html
	腾讯云	安全公告： http://bbs.qcloud.com/thread-48531-1-1.html 产品补丁： http://bbs.qcloud.com/thread-48540-1-1.html
	华为云	http://www.huaweicloud.com/about/notice_securecenter_1.html
	Azure	https://www.azure.cn/blog/2018/01/04/Securing-Azure-customers-from-CPU-vulnerability
虚拟化产品	XEN	https://xenbits.xen.org/xsa/advisory-254.html
	QEMU	安全公告： https://www.qemu.org/2018/01/04/spectre/ 非官方产品补丁： https://lists.nongnu.org/archive/html/qemu-devel/2018-01/msg00811.html

	VMware vSphere	https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html
	Citrix XenServer	https://support.citrix.com/article/CTX231390