虚拟化平台安全漏洞分析与防护研究

张鉴　唐洪玉　刘文韬

(中国电信股份有限公司研究院云安全研究所,北京 102209)

摘要: 虚拟化平台是云计算服务的核心基础设施,因此虚拟化平台的安全研究在云安全中扮演了关键角色。概述了虚拟化的典型架构和主流平台,分析了虚拟化平台安全漏洞的类型、影响及主要高危漏洞,最后对主流厂商的虚拟化安全防护系统进行分析,并提出防护解决方案。

关键词: 云安全; 虚拟化; 安全漏洞; 安全防护

1　引言

(1) 虚拟化主要架构和技术

虚拟机系统主要包括裸机型(Bare-Metal) 虚拟机(I 型) 和宿主型(Hosted) 虚拟机(II 型) ,图 1 中 VMM 即是 Hypervisor。I 型虚拟机主要应用于服务器虚拟化,如 VMware ESX\ESXi、Hyper-V、Xen、KVM 等都是典型的 I 型虚拟机; 而 II 型虚拟机主要应用于桌面虚拟化,如 VMware Workstation。结合云计算需求,虚拟化技术目前更多地应用在服务器虚拟化环境。

目前,主要的虚拟化技术包括全虚拟化(Full Virtualization) 、半虚拟化(ParaVirtualization) 和硬件辅助虚拟化(Hardware-Assisted Virtualization) 。

- 全虚拟化: VMM 向虚拟机模拟出和真实硬件完全相同的硬件环境。优点: 不用修改 Guest OS 内核; 缺点: Hypervisor 给处理器带来开销。
- 半虚拟化: VMM 需要操作系统的协助才能够完成对 x86 敏感特权指令的虚拟化。优点: 性能高,能达到与原始系统相近的性能; 缺点: 必须修改 Guest OS。
- 硬件辅助虚拟化: VMM 需要硬件的协助才能完成对硬件资源的虚拟。优点: 不用修改 Guest OS 内

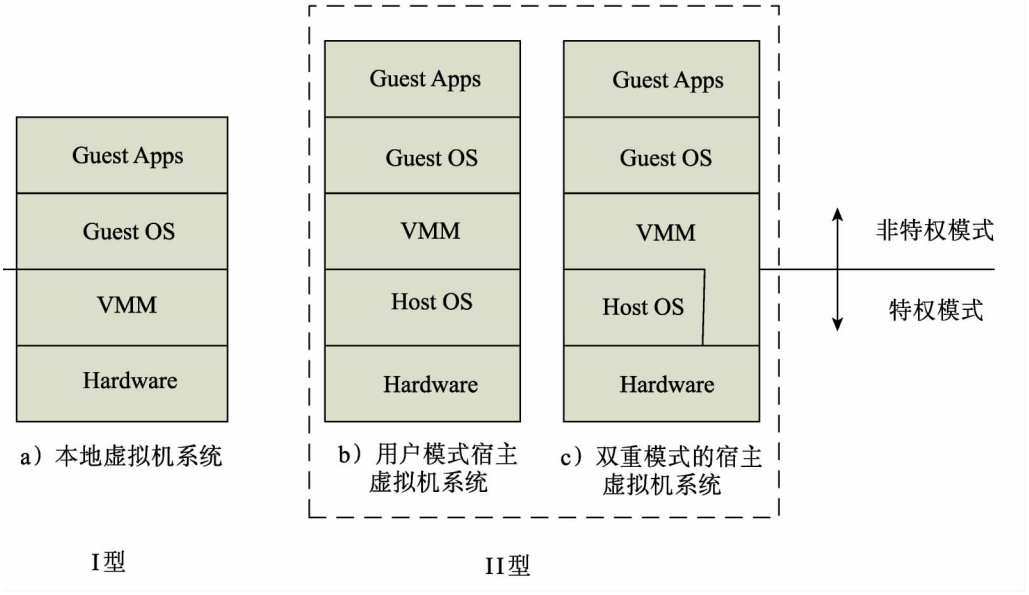

图 1　典型虚拟化架构

核; 缺点: 需要硬件支持。

(2) 主流虚拟化平台

虚拟化产品主要涉及服务器虚拟化、桌面虚拟化、应用程序虚拟化和虚拟化管理等方面。通过自身的不断发展和收购等方式,VMware、Xen 和 KVM 是目前行业的三大主流平台,其对比参见表 1。

2 虚拟化平台安全漏洞分析

2.1 安全漏洞数量分布

根据对 CVE(Common Vulnerabilities and Exposures) 安全漏洞披露信息进行查询和分析,近年来(2015—2019 年) 虚拟化相关的安全漏洞数量情况如图 2 所示。

- VMwareESXi 平台相关漏洞共 30 个,其中高危漏洞 14 个。
- KVM 平台相关漏洞共 53 个,其中高危漏洞 26 个。
- Xen 平台相关漏洞共 88 个,其中高危漏洞 41 个。

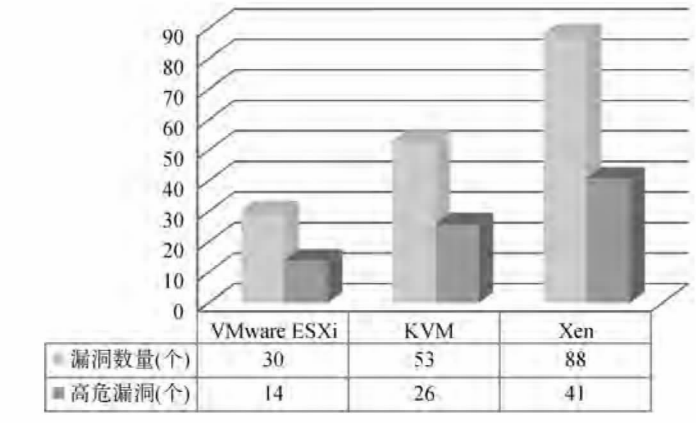

图 2 近年来主要虚拟化平台安全漏洞数量分布

2.2 安全漏洞类型和影响

对这些高危安全漏洞的风险类型进行分析,目前虚拟化平台的高危风险集中在虚拟机逃逸中,所谓虚拟机逃逸,是指在控制 Guest OS,且 Hypervisor 存在安全漏洞或配置缺陷的前提下,通过 Guest OS 来触发和利用这些漏洞。这些逃逸的实现过程都与 Hypervisor 相关,因此也可理解为 Hypervisor 逃逸。

从实际攻击的角度看,要进行逃逸攻击,需要具备 3 个条件: 某个 Guest OS 被攻击者控制; 攻击者能识别自己正处理某类型(Windows、Linux 等) 的 Guest OS 中; 能利用下层漏洞展开进一步攻击。

安全漏洞是逃逸的根源,这些漏洞存在于 Hypervisor 或设备驱动中,一般在 Guest OS 中引发。之所以将设备驱动单列出来,是由于它们可能存在于 Hypervisor 中(如 ESX 或 ESXi),也可能在 Hypervisor 之外(如 KVM 或 XEN)。显然,VMware、RedHat 和 Citrix 等厂商的 Hypervisor 在架构设计上的差异,使得相应的漏洞也需要区别分析。

(1) VMware ESXi 或 Workstation。对于 I 型 Hypervisor 而言,ESX 和 ESXi 同属于 vSphere 系列产品,但由于 ESXi 中去掉了 Service Console 这个涉及大量代码的 Linux 系统,安全隐患明显降低,事实上最近几年的安全漏洞中 VMware ESXi 的数量是最少的。

表 1 主流虚拟化平台对比

	KVM	Xen	VMware
虚拟化技术	半虚拟化、硬件辅助	半虚拟化	全虚拟化
与操作系统的关系	Linux 内核模块	操作系统之上的模块	操作系统之上的模块
HostOS	Linux(32 位,64 位)	Linux, Windows, Solaris, BSD(32 位,64 位)	Linux Windows(32 位,64 位)
使用架构和硬件平台	x86,x86_64(Intel-VT/AMD-V)	x86,x86_64,安腾,ARM	x86,x86_64,安腾,ARM
技术成熟度	高速发展中,技术先进,是未来的发展趋势	技术成熟,历史久远	商业级的技术,技术成熟,稳定性高
支持厂商	Linux 社区,RedhatUbuntu,Novell,IBM	Citrix,Oracle,Novell	EMC,VMware
企业级特性支持程度	需企业自己开发,商业级的有 Redhat 的虚拟化产品	需企业自己开发,商业级的有 Citrix 的 Xen Server	功能性能最为强大,但价格昂贵

(2) Citrix Xen。Xen 作为重要的开源 Hypervisor,其最大优点在于功能代码易于整合,因此为众多厂商所采用(如阿里云、华为云的建设都是采用的 Xen)。Xen 将设备驱动程序放在了 Domain0 中,尽管在一定程度上减少了 Hypervisor 自身漏洞,但是实际发生的漏洞依然是最多的。

(3) RedHat KVM。KVM 全称是基于内核的虚拟机(Kernel-based Virtual Machine),是一个 Linux 的一个内核模块,该内核模块使得 Linux 变成了一个 Hypervisor。从漏洞披露情况来看,KVM 的安全漏洞主要来自于 Linux 内核的安全缺陷和配置不当导致的问题。

从攻击后果上看,具体的安全漏洞类型可分为远程代码执行、DoS 攻击、权限获取、敏感信息泄露 4 类。

- 远程代码执行。在 Hypervisor 中执行任意代码(通常为 ShellCode)。在执行任意代码的基础上,可以进一步实现:安装基于 Hypervisor 的后门,著名的芯片级 Rootkit Blue Pill 便是典型例子;渗透到管理系统)、Host OS 或其它 Guest OS 中并安装 Rootkit,实现对系统的控制。

- DoS(拒绝服务)攻击。攻击者可以利用 Hypervisor 存在的安全漏洞,导致 Hypervisor 出现异常,进而使得单个甚至是所有的虚拟主机发生宕机,此种情况若出现在大型云服务提供商中,将导致非常严重的经济和社会影响。

- 权限获取。除了上述两种攻击形式外,还有一种形式,可以造成越权操作,使虚拟机攻击者可以获取 Hypervisor 或 Host OS 的权限,如 Xen 平台上的 XSA-222 漏洞(CVE-2017-10918),便是利用内存验证缺陷导致攻击者可越权获取主机权限。

- 敏感信息泄露。由于系统缺陷或配置不当,导致攻击者浏览到正常权限以外的信息,主要集中在 Xen 平台,如 CVE-2017-17045,存在 Populate on Demand (PoD) 按需填充配置不当,导致虚拟机攻击者获取宿主机敏感信息。

2.3 主要高危安全漏洞

按照上述对安全漏洞的分类,并对安全漏洞的利用方式和可能造成的危害进行深入分析,2018 年以来,主流虚拟化平台的主要高危漏洞如表 2、3、4 所示。

表 2 VMware 虚拟化平台主要高危漏洞

CVE 编号	安全风险	风险类型	影响平台
CVE-2018-6965 CVE-2018-6966 CVE-2018-6967	Shader Translator 存在越界读取漏洞,可能导致信息泄露或具有普通权限的攻击者造成虚拟机宕机	DoS 攻击	VMware ESXi (6.7 before ESXi670-201806401-BG), Workstation (14.x before 14.1.2), and Fusion (10.x before 10.1.2)
CVE-2018-6974	SVGA 设备存在越界读取漏洞,虚拟机用户可以在宿主机进行远程代码执行	远程代码执行	VMware ESXi (6.7 before ESXi670-201810101-SG, 6.5 before ESXi650-201808401-BG, and 6.0 before ESXi600-201808401-BG), Workstation (14.x before 14.1.3) and Fusion (10.x before 10.1.3)
CVE-2018-6981	vmxnet3 虚拟化网络适配器存在未初始化内存利用漏洞,虚拟机用户可以在宿主机进行远程代码执行	远程代码执行	VMware ESXi 6.7 without ESXi670-201811401-BG and VMware ESXi 6.5 without ESXi650-201811301-BG, VMware ESXi 6.0 without ESXi600-201811401-BG, VMware Workstation 15, VMware Workstation 14.1.3 or below, VMware Fusion 11, VMware Fusion 10.1.3 or below
CVE-2019-5518 CVE-2019-5519	虚拟 USB 1.1 UHCI 存在越界读写漏洞,虚拟机用户可以在宿主机进行远程代码执行	远程代码执行	VMware ESXi (6.7 before ESXi670-201903001, 6.5 before ESXi650-201903001, 6.0 before ESXi600-201903001), Workstation (15.x before 15.0.4, 14.x before 14.1.7), Fusion (11.x before 11.0.3, 10.x before 10.1.6)

表 3　KVM 虚拟化平台主要高危漏洞

CVE 编号	安全风险	风险类型	影响平台
CVE-2018-10901	GDT. LIMIT 设置不当,导致攻击者可在 GDT 中插入恶意代码,造成越权操作	权限获取	Linux kernel ' s KVM virtualization subsystem
CVE-2018-16882	KVM Hypervisor 存在 use-after-free(释放后可重用) 漏洞,可导致虚拟机攻击者获取宿主机权限或发动 DoS 攻击	权限获取 DoS 攻击	Kernel versions before 4. 14. 91 and before 4. 19. 13
CVE-2019-6974	virt/kvm/kvm_main. c 存在 use-after-free(释放后可重用) 漏洞,可导致虚拟机攻击者获取宿主机权限或发动 DoS 攻击	权限获取 DoS 攻击	Linux kernel before 4. 20. 8

表 4　Xen 虚拟化平台主要高危漏洞

CVE 编号	安全风险	风险类型	影响平台
CVE-2018-19966	Shadow 分页的数据结构存在安全漏洞,可导致虚拟机攻击者获取宿主机权限或发动 DoS 攻击	权限获取 DoS 攻击	Xen through 4. 11
CVE-2018-18883	nested VT-x 权限设置不当,可导致虚拟机攻击者获取宿主机权限或发动 DoS 攻击	权限获取 DoS 攻击	Xen 4. 9. x through 4. 11. x
CVE-2018-14678	arch/x86/entry/entry_64. S 存在安全漏洞,可导致虚拟机攻击者获取宿主机权限或发动 DoS 攻击	权限获取 DoS 攻击	Linux kernel through 4. 17. 11, as used in Xen through 4. 11. x
CVE-2018-10982	存在 vHPET 中断注入漏洞,可导致虚拟机攻击者获取宿主机权限或发动 DoS 攻击	权限获取 DoS 攻击	Xen through 4. 10. x

3　虚拟化平台安全防护

保障虚拟化平台安全性是一个系统性工程,需要针对虚拟化平台的技术特点,综合考虑 Hypervisor 和虚拟化主机防护措施,才能充分保障虚拟化平台安全。目前,主流厂商的技术路线基本一致,都是以虚拟主机+agent 协同的方式来实现虚拟化平台的安全防护。

3.1　瑞星虚拟化安全方案

瑞星虚拟化平台安全防护系统由管理中心、升级中心、日志中心、扫描服务器、安全虚拟设备、安全终端 Linux 杀毒和安全防护终端等子系统组成。各子系统均包括若干不同的模块,除承担各自的任务外,还与其它子系统通讯,协同工作,共同完成企业内部的安全防护。

(1) 管理中心: 作为管控服务器,一方面为管理员提供 B/S 方式的管理界面交互; 另一方面,负责为客户端提供策略、任务、授权等业务数据。

(2) 升级中心: 在企业内部为所有客户端提供 HTTP 式升级服务,以减轻客户端对互联网的依赖,支持手动与自动升级方式。

(3) 日志中心: 接收各客户端产生的日志数据,统一进行入库操作,并负责各客户端的数据同步。

(4) 扫描服务器: 独立的子产品,提供云端查杀服务。

(5) 安全虚拟设备: 存在于每一台虚拟主机上(如 ESXi) ,为每一台无代理虚拟机提供安全防护服务,不需要再安装安全产品。

(6) 终端防护与 Linux 防御: 终端安全类子产品,支持 Windows 与 Linux 系统,主要安装在物理机上,也支持安装在虚拟机上,此时将接管无代理安全防护。

3.2　奇安信虚拟化安全方案

奇安信的虚拟化安全管理系统,能够对物理资源池、虚拟资源池、云端资源池进行统一的安全防护与管理,并且具备对混合虚拟化平台、混合操作系统、混合系统应用环境的兼容能力。

(1) 多平台统一管理

虚拟化安全管理系统支持主流 VMware、Xen 和

KVM 平台,可同时支持 Windows 与 Linux 版本并统一管理,同时在全球首个推出支持 Linux 系统无代理部署方式。

(2) Hypervisor 层防护

Hypervisor 多基于 Linux 系统开发,继承了 Linux 系统的安全风险。攻击机能够利用上层虚拟机漏洞,向下攻破 Hypervisor,从而造成虚拟机逃逸或整个虚拟化平台的崩溃。依托虚拟化攻防团队的多年的研究成果,虚拟化安全管理系统为客户提供了 Hypervisor 层的防护功能,保障了整个虚拟化核心层的安全。

(3) 全面支持国产化虚拟平台和操作系统

虚拟化安全管理平台除了支持 VMware、Citrix、微软等国外虚拟化平台之外,也实现了对国产虚拟化厂商的全面支持,如华为、新华三、浪潮、中兴、青云、Easystack、航天云宏等。另外,对中标麒麟、红旗、深度等国产操作也实现了全面兼容。

4 结束语

虚拟化平台是当前云计算的核心基础设施,云计算技术都会利用虚拟化平台实现在同一台物理机上运行多台虚拟机,从而充分利用资源。而虚拟化平台如果出现安全风险,轻则影响单个用户的体验,重则会影响到整个云平台的运行。本文从虚拟化的典型架构和主流平台入手,深入分析了虚拟化平台安全漏洞的类型、影响及主要高危漏洞,最后对主流厂商虚拟化安全防护系统进行了分析,提出防护解决方案,希望能对云安全防护体系的建设和推进提供有益的技术参考。

参考文献

[1] 奇安信. 虚拟化安全管理系统[EB/OL]. [2019-12-10]. https://www.qianxin.com/product/virtualization_security.

[2] 张鉴,冯晓东,唐洪玉.5G 网络 NFVI 安全防护架构[J].移动通信,2019,43(10):43-48.

[3] 张鉴,唐洪玉,张静. 中国电信云计算业务平台安全建设探讨[J]. 电信技术,2017(06):57-61.

作者简介:

张鉴 中国电信股份有限公司网络与信息安全研究院云安全研究所高级工程师,主要研究方向为云安全、安全攻防、5G 安全

唐洪玉 中国电信股份有限公司网络与信息安全研究院云安全研究所所长,高级工程师,主要研究方向为云安全、态势感知、威胁情报

刘文韬 中国电信股份有限公司网络与信息安全研究院云安全研究所工程师,主要研究方向为云安全、威胁情报

Security vulnerability analysis and protection research of virtualization platform

ZHANG Jian, TANG Hongyu, LIU Wentao

(Institute of cloud security, China telecom Corporation Limited research institute, Beijing 102209, China)

Abstract: The virtualization platform is the core infrastructure of cloud computing services, therefore, security research for virtualization platform plays a key role in cloud security. This paper first summarizes the typical architecture and mainstream platform of virtualization, then deeply analyzes the types, impacts and major high-risk events of virtualization platform security vulnerabilities, finally analyzes the virtualization security protection system of mainstream manufacturers and puts forward protection solutions.

Key words: cloud security; virtualization; security vulnerability; security protection

(收稿日期: 2019-12-30)