安全事件通告

VMWare 虚拟环境逃逸漏洞通告

360CERT
北京奇虎科技有限公司 | 2020-11-25

报告信息

报告名称	VMWare 虚拟环境逃逸漏洞通告		
报告类型	安全事件通告	**报告编号**	B6-2020-112501
报告版本	1	**报告日期**	2020-11-25
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2020-11-25	360CERT	360CERT	撰写报告

目录

一、 事件档案

漏洞类型	缓冲区/栈溢出漏洞
CVE 编号	CVE-2020-4004 等
相关厂商	Vmware
相关组件	esxi 等
威胁等级	高危
影响面	一般
360CERT 评分	8.8
修复方案	通用修补方案/临时修补方案
事件发布时间	2020-11-25
报告生成时间	2020-11-25

二、事件简述

2020 年 11 月 25 日，360CERT 监测发现 VMWare 发布了 VMSA-2020-0026 的风险通告，漏洞编号为 CVE-2020-4004,CVE-2020-4005 ，事件等级：高危，事件评分：8.8。

VMWare 发布缓冲区溢出、权限提升两处漏洞

本地具有管理员权限的攻击者通过执行特制的二进制程序，可造成虚拟环境逃逸，并控制宿主主机/服务器。

两处漏洞均由 Qihoo 360 Vulcan Team 在天府杯向 VMWare 提交

对此，360CERT 建议广大用户及时将 VMware 软件 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

三、 事件评级

经过安全技术人员的分析，最终对该事件的评定结果如下

评定方式	等级
威胁等级	高危
影响面	一般
360CERT 评分	8.8

四、 事件详情

CVE-2020-4004: 缓冲区/栈溢出漏洞

VMware ESXi，Workstation 和 Fusion 在 XHCI USB 控制器(用于 USB3.x 协议接入)中包含一个 Use-After-Free 漏洞。本地具有管理员权限的攻击通过执行特制的二进制程序，可造成虚拟环境逃逸，并取得宿主主机/服务器控制权限。

CVE-2020-4005: 权限提升漏洞

VMware ESXi 存在一处特权升级漏洞。本地具有 VMX 进程控制权限的攻击者通过执行特制的二进制程序，可在受影响的系统上获得权限提升（VMX 进程权限提升到本地管理员）。该漏洞可和 CVE-2020-4004 进行组合利用，最终控制宿主主机/服务器

五、 影响版本

产品名称	影响版本
esxi	6.5/6.7/7.0
fusion	11.x
workstation	15.x
vmware_cloud_foundation	3.x/4.x

六、 漏洞列表

编号	描述	导致结果	威胁等级
CVE-2020-4004	缓冲区/栈溢出漏洞	任意代码执行	高危
CVE-2020-4005	权限提升漏洞	权限提升	高危

七、 安全建议

(一) 通用修补方案

根据 VMWare 官方通告进行修复

VMWare VMSA-2020-0026-修复建议:

https://www.vmware.com/security/advisories/VMSA-2020-0026.html

(二) 临时修补方案

根据 VMWare 官方通告移除 XHCI 控制器能够有效的缓解漏洞影响

VMWare 移除 XHCI 控制器手册:

https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-ACA30034-EC88-491B-8D8B-4E319611C308.html

八、 产品侧解决方案

(一) 360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或(shaoyulong#360.cn)获取对应产品。

九、 参考链接

1. VMSA-2020-0026

   https://www.vmware.com/security/advisories/VMSA-2020-0026.html

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危