关于 VMware 虚拟环境逃逸漏洞的紧急预警

深圳市网络与信息安全信息通报中心

2020 年 11 月 25 日

编号：2020064

目录

一、安全预警

近期，发现VMware系列软件存在虚拟环境逃逸漏洞（CNNVD编号：CNNVD-202011-1762、CNNVD-202011-1764）。VMware ESXi是一套可直接安装在物理服务器上的服务器虚拟化平台，VMware Fusion是一套专用于在苹果机（Mac）上运行Windows应用程序的的虚拟机软件，VMware Workstation是一套虚拟机软件，VMware Cloud Foundation是一套一体化混合云平台。应用范围较广，因此威胁影响范围较大。

请各重点单位高度重视，加强网络安全防护，切实保障网络系统安全稳定运行。

二、事件信息

（一）事件概要

事件名称	VMware 虚拟环境逃逸漏洞 CNNVD 编号： CNNVD-202011-1762、CNNVD-202011-1764		
威胁类型	缓冲区溢出 权限提升	**威胁等级**	高
受影响的应用版本			
• VMware esxi 6.5/6.7/7.0 • VMware fusion 11.x • VMware workstation 15.x • VMware cloud_foundation3.x/4.x			

（二）漏洞描述

- VMware 缓冲区/栈溢出漏洞（CNNVD 编号：CNNVD-202011-1762）

VMware ESXi、Workstation 与 Fusion 产品的 XHCI USB 控制器中存在一处 Use-After-Free 漏洞。具有管理员权限的攻击者可以通过在本地执行特制的二进制程序，造成虚拟环境逃逸，并取得宿主主机/服务器控制权限。

- VMware 权限提升漏洞（CNNVD 编号：CNNVD-202011-1764）

VMWare ESXi 等多个组件存在权限提升漏洞，攻击者执行精心构造的二进制文件可以将用户由 vmx 执行权限提升为系统管理员权限。该漏洞可以与 CNNVD-202011-1762 组合利用，最终取得宿主主机/服务器控制权限。

（三）影响范围

- VMware esxi 6.5/6.7/7.0
- VMware fusion 11.x
- VMware workstation 15.x
- VMware cloud_foundation3.x/4.x

三、处置建议

（一）解决方案

VMware 官方已经提供解决方案，参考链接如下：

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

四、应急处置建议

一旦发现系统中存在漏洞被利用的情况，要第一时间上报我中心（电话：84452816），同时开展以下紧急处置：

一是立即断开被入侵的主机系统的网络连接，防止进一步危害；

二是留存相关日志信息；

三是通过“解决方案”加固系统并通过检查确认无相关漏洞后再恢复网络连接。