关于 VMWare 命令注入漏洞的紧急预警

深圳市网络与信息安全信息通报中心

2020 年 12 月 08 日

编号：2020068

目录

一、安全预警

近期，发现VMWare存在命令注入漏洞（CNNVD编号：CNNVD-202011-1790），VMWare Identity Manager（简称vIDM)是VMware开发的一套身份管理系统。用户利用这套系统可以实现企业级应用的单点登录,可以在各种设备上访问企业在私有数据中心或者公有云平台上的应用或者数据。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 命令注入漏洞 CNNVD 编号：CNNVD-202011-1790		
威胁类型	命令注入	**威胁等级**	高
受影响的应用版本			
• VMware Workspace ONE Access 20.01, 20.10 • VMware Identity Manager 3.3.1-3.3.3 • VMware Identity Manager Connector 3.3.1-3.3.3 • VMware Identity Manager Connector 19.03.0.0, 19.03.0.1			

（二）漏洞描述

攻击者利用此漏洞可以在受影响主机上以管理员权限执行代码。

利用漏洞必须访问 web 端的管理界面，并且需要对 TLS 加密的管理接口进行基于身份验证的口令访问，使用强且唯一的口令可以降低被利用的可能性，但无法降低已产生的危害。如果 web 界面无法从公开网络中访问则风险进一步降低。该接口通常在 8

443 端口上运行。由于服务器在安装时需要输入口令，因此没有已知的默认口令。

（三）影响范围

- VMware Workspace ONE Access 20.01，20.10
- VMware Identity Manager 3.3.1-3.3.3
- VMware Identity Manager Connector 3.3.1-3.3.3
- VMware Identity Manager Connector 19.03.0.0，19.03.0.1

三、处置建议

（一）解决方案

官方已经提供最新补丁，参考链接如下：

https://kb.vmware.com/s/article/81731

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。