河南省教育信息安全中心

VMware 公司相关产品存在安全漏洞预警

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2021 年 03 月 09 日

关于 VMware 公司相关产品存在安全漏洞预警

事件描述

近日，据有关部门通报，VMware 公司相关产品存在多个安全漏洞，包括 VMware vSphere Client 安全漏洞（CNNVD-202102-1566、CVE-2021-21972）、VMware ESXi 安全漏洞（CNNVD-202102-1560、CVE-2021-21974）。

VMware vSphere Client 安全漏洞（CNNVD-202102-1566、CVE-2021-21972）介绍：

VMware vSphere Client 是美国威睿（VMware）公司的一个应用软件，提供虚拟化管理。VMware vSphere Client 存在一个安全漏洞，未授权的攻击者可以通过开放 443 端口的服务器向 vCenter Server 发送精心构造的请求，从而在目标系统上远程执行恶意代码。

VMware ESXi 安全漏洞（CNNVD-202102-1560、CVE-2021-21974）介绍：

VMware ESXi 是美国威睿（VMware）公司的一套可直接安装在物理服务器上的服务器虚拟化平台。VMware ESXi 存在一个安全漏洞，攻击者与 ESXi 处于同一网段且可以访问 427 端口时，可以通过向 427 端口发送恶意请求包触发 OpenSLP 服务中的堆溢出漏洞，最终造成远程代码执行。

影响范围

vSphere Client 6.5
vSphere Client 6.7
vSphere Client 7.0
VMware Cloud Foundation（vCenter Server）3.x
VMware Cloud Foundation（vCenter Server）4.x
ESXi 6.5
ESXi 6.7
ESXi 7.0
VMware Cloud Foundation (ESXi)3.X
VMware Cloud Foundation (ESXi)4.X

处置建议

官方已经发布新版本修复该漏洞，详细信息如下：
https://www.vmware.com/security/advisories/VMSA-2021-0002.html

鉴于该漏洞影响范围较大，潜在危害程度较高，各单位要及时通知相关用户，核查 VMware 公司相关产品使用情况，修补漏洞，消除安全隐患。