网络安全风险预警通报

2021 年第 1 期 （总第 13 期）

广西大学网络信息中心 2021 年 6 月 9 日

【预警类型】 高危预警

【预警内容】

VMware vCenter Server 存在远程代码执行漏洞的安全公告

安全公告编号 CNTA-2021-0020

一、漏洞概述

VMware vSphere 是美国威睿公司推出一套服务器虚拟化解决方案，包括虚拟化、管理和界面层。VMware vSphere 的两个核心组件是 ESXi 服务器和 vCenter。VMware ESXi 是 VMware 的裸机虚拟机管理程序，用以创建运行虚拟机和虚拟设备。VMware vCenter Server 是管理整个 VMware 虚拟化基础架构的软件，用于集中管理多个 ESXi 主机和以及在 ESXi 主机上运行的虚拟机。用户可以通过 vSphere Client 登录

到 vCenter Server 来管理 vSphere 清单，使用 vSphere Client 需要 Web 浏览器支持。

攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞相关细节尚未公开，VMware 公司已发布新版本修复漏洞，建议用户尽快更新至最新版本。

二、漏洞详情

2021 年 5 月 25 日，VMware 公司发布多个关于 vCenter Server 的安全公告，其中包括 VMware vCenter Server 存在远程代码执行漏洞。该漏洞存在于 vSphere Client(HTML5)包含的运行状况检查插件 vSAN(Virtual San Health Check)中，该插件在 vCenter Server 中默认启用。由于缺乏必要的输入验证,攻击者可以向开放 443 端口的 vCenter Server 服务器发送恶意构造的请求，在目标系统上执行任意代码，获得目标服务器的权限，实现对 vCenter Server 的远程代码执行。

三、漏洞影响范围

漏洞影响的产品版本包括：

VMware vCenter Server 7.0

VMware vCenter Server 6.7

VMware vCenter Server 6.5

Cloud Foundation (vCenter Server) 4.x

Cloud Foundation (vCenter Server) 3.x

四、漏洞处置建议

目前，VMware 公司已发布新版本修复上述漏洞，CNVD 建议用户立即升级至最新版本：

https://www.vmware.com/security/advisories/VMSA-2021-0010.html

附：参考链接：

https://www.vmware.com/security/advisories/VMSA-2021-0010.html