关于 VMware 多款产品存在远程代码执行漏洞的预警通知

校属各单位：

根据上级部门监测发现，攻击者利用 VMware vCenter Server 远程代码执行漏洞（CNVD-2021-12322，对应 CVE-2021-21972）和 VMware ESXi OpenSLP 堆溢出漏洞（CNVD-2021-12321，对应 CVE-2021-21974），可在未授权的情况下远程执行代码。目前，部分漏洞细节和利用代码已公开，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进行修复。

一、漏洞情况分析

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。

2021 年 2 月 23 日，VMware 公司发布漏洞安全公告，VMware 多个组件存在远程代码执行、堆溢出漏洞和信息泄露漏洞的高危漏洞。1）VMware vCenter Server 远程代码执行漏洞。未经身份验证的攻击者利用该漏洞，通过向目标主机的 443 端口发送恶意构造请求，写入后门文件，进而在托管 vCenterServer 的操作系统上实现远程代码执行。2）VMware ESXi OpenSLP 堆溢出漏洞。与 ESXi 宿主机处于同一网段、未经身份验证的攻击者利用该漏洞，通过向目标主机的 427 端口发送恶意构造请求，触发 OpenSLP 服务基于堆的缓冲区溢出，导致远程代码执行。

二、漏洞影响范围

漏洞影响的产品版本包括：

VMware vCenter Server 6.5

VMware vCenter Server 6.7

VMware vCenter Server 7.0

VMware ESXi 6.5

VMware ESXi 6.7

VMware ESXi 7.0

三、漏洞处置建议

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

https://www.vmware.com/security/advisories/VMSA-2021-0002.html

请各单位立即组织专业力量对管理的设备开展网络安全风险排查，及时更新漏洞补丁，消除安全隐患。

特此通知。

联系人：侯国平，联系电话：65362000

信息技术中心

2021 年 2 月 26 日