

【内部】

关于虚拟机管理软件（VMware ESXi）存在 高危漏洞的风险提示

VMware ESXi 是美国威睿公司推出的一款虚拟机管理软件，用以创建运行虚拟机和虚拟设备。近日以 VMware ESXi 服务器为目标的大规模勒索软件攻击正在席卷全球，包括法国、芬兰、加拿大、美国、意大利等多个国家数千台服务器遭到入侵。攻击者利用了 2021 年 2 月公开的高危漏洞

（CNVD-2021-12321，

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-12321>），

该漏洞详情如下：

攻击者可以向 VMware ESXi 软件目标服务器 427 端口发送恶意构造的数据包，从而触发其 OpenSLP 服务堆缓冲区溢出，并执行任意代码。

该漏洞影响范围为：

VMware ESXi70U1c-17325551 7.0 版本

VMware ESXi670-202102401-SG 6.7 版本

VMware ESXi650-202102101-SG 6.5 版本

请各单位高度重视，采取措施加强防范，排查是否安全隐患。若发生网络安全事件，各单位需按照相关网络安全事件应急预案的要求，及时处置并报告上级主管部门。

2023 年 2 月 23 日