网络安全预警通报

2025 年第 1 期 （总第 51 期）

西安交通大学网络信息中心 2025 年 3 月 8 日

【预警类型】高危预警

【预警内容】

VMware ESXi 虚拟机逃逸漏洞紧急风险通告

一、漏洞概述

VMware ESXi 产品中曝出高危虚拟机逃逸漏洞 CVE-2025-22224（CVSSv3.1 评分 9.3），攻击者可利用虚拟机客户机管理员权限触发 VMCI 组件堆溢出漏洞，突破沙盒隔离机制，在宿主机上执行任意代码，该漏洞已被野外攻击者积极利用。

二、漏洞详情

1.技术原理

漏洞类型：VMCI 组件的 TOCTOU（Time-of-Check Time-of-Use）竞争条件漏洞，导致越界写入。

攻击路径：攻击者通过虚拟机客户机（VM Guest）管理员权限，构造恶意堆溢出操作；触发宿主机 VMX 进程权限逃逸，执行系统级代码。

2.利用条件

必要条件：已获取虚拟机客户机的管理员或 root 权限。

关联风险：攻击链可能结合 CVE-2025-22225（权限提升）和 CVE-2025-22226（内存泄露）进行组合利用。

三、漏洞影响范围

1.VMware ESXi 受影响版本：

ESXi 8.0（全版本）

ESXi 7.0（全版本）

2.VMware Workstation 受影响版本：

Workstation Pro/Player 全版本（包括最新版本）

3.VMware Fusion 受影响版本：

Fusion 全版本（包括最新版本）

4.VMware 云平台受影响产品：

VMware Cloud Foundation（全版本）

VMware Telco Cloud Platform（全版本）

四、漏洞缓解措施

1.权限管控

1）限制虚拟机客户机管理员权限：禁止非必要账号获取客户机 root 或管理员权限，并定期审计权限分配记录。

2)禁用高危操作:关闭虚拟机内非必需的硬件驱动(如虚拟化增强工具)、调试接口及 VMCI 组件的部分高危功能。

2．隔离策略

网络隔离：

1) 将未修复的 ESXi 主机迁移至独立 VLAN，限制其与生产环境的通信。

2）禁用宿主机管理接口（如 vSphere Client）的互联网暴露端口（默认 443/TCP）。

3）服务关闭：若无法升级，立即关闭虚拟化服务（执行 /etc/init.d/vpxastop 停止 VPX 代理）。

3．修复限制与历史经验

1）强制完整升级：该漏洞无法通过 VMware 的 Live Patch 热修复，必须执行完整系统升级；

2）补丁验证流程：参考 CVE-2024-22235 修复案例，在非生产环境模拟攻击验证补丁有效性；

官方参考链接：

（https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24264）

3）确保升级后测试虚拟机迁移、HA 等高可用性功能。

4.官方补丁资源

官方公告：完整修复版本清单及补丁下载详见

（https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390）