



河南省教育信息安全监测中心

VMware vCenter Server 权限提升漏洞

预警



VMware vCenter Server 权限提升漏洞预警

事件描述

近期，VMware 官方发布了 vCenter Server 权限提升的风险通告，漏洞编号为 CVE-2021-22048，漏洞等级：高危。vCenter Server 在 IWA（集成 Windows 身份验证）身份验证机制中包含一个提权漏洞，对 vCenter Server 具有非管理访问权限的黑客可能会利用此问题将特权提升到更高特权组。

影响范围

VMware vCenter Server 6.5

VMware vCenter Server 6.7

VMware vCenter Server 7.0

VMware Cloud Foundation 3.x

VMware Cloud Foundation 4.x

安全建议

1、目前 VMware 暂未发布此漏洞的补丁，但 VMware 提供了该漏洞的修复方案，将 SSO 身份源配置从集成 Windows 身份验证（IWA）切换到以下选项之一：

- 1) Active Directory over LDAPs 身份验证
- 2) AD FS 的身份提供者联合（仅限 vSphere 7.0）

详细信息可参考 <https://kb.vmware.com/s/article/86292>，必要时联系厂商协助处理。

2、对 VMware vCenter 等关键服务增加访问控制，尽可能限定内网访问。

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052