



# 河南省教育信息安全中心

## VMware 公司相关产品存在安全漏洞预警



# 关于 VMware 公司相关产品存在 安全漏洞预警

## 一、事件描述

2021年9月21日,VMware官方发布了安全公告,修复了多个vCenter Server的高危漏洞,其中包括文件上传漏洞(CVE-2021-22005)、本地提权漏洞(CVE-2021-21991)、反向代理绕过漏洞(CVE-2021-22006)、服务端API鉴权漏洞(CVE-2021-22011)、本地提权漏洞(CVE-2021-22015)、未经身份验证的API信息泄露漏洞(CVE-2021-22012)、vCenter Server文件路径遍历漏洞(CVE-2021-22013)、vCenter Server反映了XSS漏洞(CVE-2021-22016)、rhttpproxy绕过漏洞(CVE-2021-22017)、经过身份验证的代码执行漏洞(CVE-2021-22014)、vCenter Server文件删除漏洞(CVE-2021-22018)、vCenter Server XML解析拒绝服务漏洞(CVE-2021-21992)、vCenter Server本地信息泄露漏洞(CVE-2021-22007)、vCenter Server拒绝服务漏洞(CVE-2021-22019)、vCenter Server VAPI多重拒绝服务漏洞(CVE-2021-22009)、vCenter Server VPXD拒绝服务漏洞(CVE-2021-22010)、vCenter Server信息泄露漏洞(CVE-2021-22008)、vCenter Server Analytics服务拒绝服务漏洞(CVE-2021-22020)、服务器端请求伪造漏洞(CVE-2021-21993)。

## 二、影响范围

vSphere 7.0

产品	版本	运行平台	CVE 编号	严重性	已修复版本
vCenter Server	7.0	Any	CVE-2021-22005	危急	7.0 U2c
vCenter Server	7.0	Any	CVE-2021-21991, CVE-2021-21992, CVE-2021-21993, CVE-2021-22006, CVE-2021-22007, CVE-2021-22008, CVE-2021-22009, CVE-2021-22010, CVE-2021-22014, CVE-2021-22015, CVE-2021-22019, CVE-2021-22020	重要	7.0 U2c
vCenter Server	7.0	Any	CVE-2021-22011, CVE-2021-22018	重要	7.0 U2d
vCenter Server	7.0	Any	CVE-2021-22012, CVE-2021-22013, CVE-2021-22016, CVE-2021-22017	N/A	不受影响
Cloud Foundation (vCenter Server)	4.x	Any	CVE-2021-22005	危急	KB85718 (4.3)

Cloud Foundation (vCenter Server)	4. x	Any	CVE-2021-21991, CVE-2021-21992, CVE-2021-21993, CVE-2021-22006, CVE-2021-22007, CVE-2021-22008, CVE-2021-22009, CVE-2021-22010, CVE-2021-22014, CVE-2021-22015, CVE-2021-22019, CVE-2021-22020	重要	KB85718 (4.3)
Cloud Foundation (vCenter Server)	4. x	Any	CVE-2021-22011, CVE-2021-22018	重要	KB85718 (4.3.1)
Cloud Foundation (vCenter Server)	4. x	Any	CVE-2021-22012, CVE-2021-22013, CVE-2021-22016, CVE-2021-22017	N/A	不受影响

vSphere 6.7

产品	版本	运行平台	CVE 编号	严重性	已修复版本
vCenter Server	6.7	Virtual Appliance	CVE-2021-22005	危急	6.7 U3o
vCenter Server	6.7	Windows	CVE-2021-22005	N/A	不受影响
vCenter Server	6.7	Any	CVE-2021-21991, CVE-2021-21992, CVE-2021-21993, CVE-2021-22006, CVE-2021-22008, CVE-2021-22009, CVE-2021-22010, CVE-2021-22011, CVE-2021-22016, CVE-2021-22017	重要	6.7 U3o
vCenter Server	6.7	Virtual Appliance	CVE-2021-22007, CVE-2021-22015, CVE-2021-22014, CVE-2021-22019, CVE-2021-22020	重要	6.7 U3o
vCenter Server	6.7	Windows	CVE-2021-22007, CVE-2021-22014, CVE-2021-22015, CVE-2021-22019, CVE-2021-22020	N/A	不受影响
vCenter Server	6.7	Any	CVE-2021-22012, CVE-2021-22013, CVE-2021-22018	N/A	不受影响
Cloud Foundation (vCenter Server)	3. x	Any	CVE-2021-22005	危急	KB85719 (3.10.2.2)
Cloud Foundation (vCenter Server)	3. x	Any	CVE-2021-21991, CVE-2021-21992, CVE-2021-21993, CVE-2021-22006, CVE-2021-22007, CVE-2021-22008,	重要	KB85719 (3.10.2.2)

Server)			CVE-2021-22009, CVE-2021-22010, CVE-2021-22011, CVE-2021-22014, CVE-2021-22015, CVE-2021-22016, CVE-2021-22017, CVE-2021-22019, CVE-2021-22020		
Cloud Foundation (vCenter Server)	3. x	Any	CVE-2021-22012, CVE-2021-22013, CVE-2021-22018	N/A	不受影响

### vSphere 6.5

产品	版本	运行平台	CVE 编号	严重性	已修复版本
vCenter Server	6.5	Any	CVE-2021-21991, CVE-2021-21992, CVE-2021-21993, CVE-2021-22008, CVE-2021-22009, CVE-2021-22011, CVE-2021-22017	重要	6.5 U3q
vCenter Server	6.5	Virtual Appliance	CVE-2021-22012, CVE-2021-22013, CVE-2021-22014, CVE-2021-22015, CVE-2021-22019	重要	6.5 U3q
vCenter Server	6.5	Windows	CVE-2021-22012, CVE-2021-22013, CVE-2021-22014, CVE-2021-22015, CVE-2021-22019	N/A	不受影响
vCenter Server	6.5	Any	CVE-2021-22005, CVE-2021-22006, CVE-2021-22007, CVE-2021-22010, CVE-2021-22016, CVE-2021-22018, CVE-2021-22020	N/A	不受影响

## 三、处置建议

1、根据 vCenter 版本及所部属的环境，参考官方指引升级相关产品至安全版本，官方链接如下：

<https://www.vmware.com/security/advisories/VMSA-2021-0020.html>

2、配置访问控制策略，避免受影响产品暴露在互联网。

鉴于该漏洞影响范围较大，潜在危害程度较高，各单位要及时通知相关用户，核查 VMware 公司相关产品使用情况，修补漏洞，消除安全隐患。

## 四、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](mailto:hercert@ha.edu.cn)

邮编: 450052