VMware vRealize Business for Cloud 远程代码执行漏洞 CVE-2021-21984

2021 年 5 月 6 日

一、漏洞概要

漏洞名称	VMware vRealize Business for Cloud 远程代码执行漏洞 CVE-2021-21984
组件名称	VMware vRealize Business for Cloud
影响范围	VMware vRealize Business for Cloud < 7.6.0
漏洞类型	远程代码执行
利用条件	1、用户认证：不需要用户认证 2、触发方式：远程
综合评价	<综合评定利用难度>：未知，PoC 未公开。 <综合评定威胁等级>：高危，能造成远程代码执行。

二、漏洞分析

2.1 组件介绍

VMware vRealize Business（前称为 ITBusinessManagementSuite）是美国威睿（VMware）公司的一款可用于直观了解和控制云计算环境和 IT 服务成本的工具。

2.2 漏洞描述

2021 年 5 月 6 日，深信服安全团队监测到 VMware 官方发布了一则漏洞安全通告，通告披露了 VMware vRealize Business for Cloud 组件存在远程代码执行漏洞，漏洞编号：CVE-2021-21984，漏洞威胁等级：严重。

该漏洞是由于 VMware vRealize Business for Cloud 组件中存在一处未授权问题，攻击者可利用该漏洞在未授权的情况下，构造恶意数据并发起远程代码执行攻击，最终获取服务器最高权限。

三、影响范围

VMware vRealize Business for Cloud 可能受漏洞影响的资产广泛分布于世界各地，国内主要分布在北京、江苏等省市。

目前受影响的 VMware vRealize Business for Cloud 版本：

VMware vRealize Business for Cloud < 7.6.0

四、解决方案

4.1 修复建议

1.官方修复建议

当前官方已发布最新版本，建议受影响的用户及时更新升级到最新版本。链接如下：

https://kb.vmware.com/s/article/83475

打补丁/升级方法：

1. 从 VMware 下载页面下载 vRealize Business for Cloud 7.6.0 安全补丁程序 ISO 文件。

注意：选择 vRealize Business for Cloud 作为产品，然后选择 7.6.0 作为版本，然后单击 Search。

选择下面的选项。

发布名称	发布日期	内部编号	文件名
vRealize Business for Cloud 7.6安全版本	2021年5月5日	17828140	vRealize-Business-for-Cloud-7.6.0.46000-17828140-updaterepo.iso

2. 将 vRealize Business for Cloud 服务器设备 CD-ROM 驱动器连接到您下载的 ISO 文件。

3. 使用根凭据登录到 vRealize Business for Cloud 的 VAMI 门户。

4. 单击 VAMI UI 的“更新”选项卡。

5. 单击更新选项卡下的设置。

6. 选择“更新存储库”下的“使用 CDROM 更新”，然后在上传

ISO 文件和“保存设置”的位置安装路径。

7. 单击“状态”选项卡下的“安装更新”以升级到此版本。

五、时间轴

2021/5/5　深信服监测到 VMware 官方发布安全补丁。

2021/5/6　深信服千里目安全实验室发布漏洞通告。

六、了解更多

深信服千里目安全实验室持续紧跟国内外漏洞威胁情报，从中筛选出能给客户带来威胁的漏洞，第一时间推送解决方案，持续提供可感知的安全感。在这场永不停歇的攻防战争中，深信服千里目安全实验掌握一手漏洞情报，坚持“千里之外，洞悉风险”，与各大网络安全厂商一同维护网络安全，构建平衡、和谐的网络生态系统。关注深信服千里目安全实验室微信公众号，第一时间了解更多漏洞情报。