Re: AnyDesk Public Exploit Disclosure - Arbitrary file write by symbolic link attack lead to denial-of-service attack on local machine

From: chan chan <siuchunc.03 () gmail com>
Date: Sat, 16 Jul 2022 00:39:17 +0800

Hi FullDisclosure,

May I know if there is any update?
Please note that Mitre has assigned and reserved a CVE number
"CVE-2022-32450" for this vulnerability.

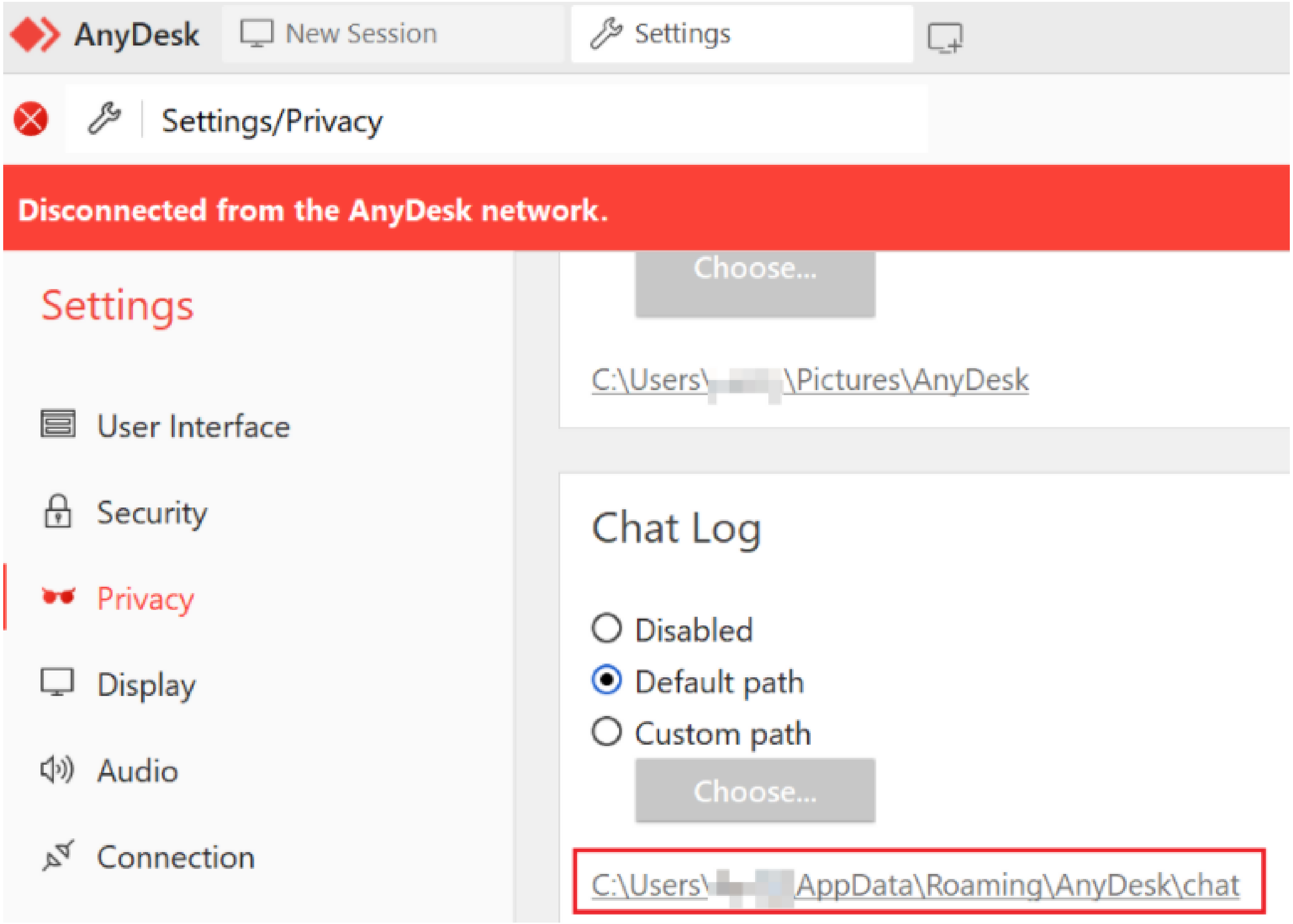
Regards,
Erwin

chan chan <siuchunc.03 () gmail com> 於 2022年6月22日週三 下午5:42寫道:

> Hi FullDisclosure,
>
> I would like to publish an exploit that I found on AnyDesk as follows.
>
> # Exploit Title: AnyDesk allow arbitrary file write by symbolic link attack lead to
> denial-of-service attack on local
> machine
> # Google Dork: [if applicable]
> # Date: 24/5/2022
> # Exploit Author: Erwin Chan
> # Vendor Homepage: https://anydesk.com/en
> # Software Link: https://anydesk.com/en
> # Version: 7.0.9
> # Tested on: Windows 11
>
> It was found that AnyDesk (version 7.0.9) was vulnerable to arbitrary file
> write by symbolic link attack leading to denial-of-service attack on local
> machine. It was noted that two functions were affected.
> *Affected function A*
> When there was a remote connection come in, a directory under AppData of
> current user (without admin privilege) and a "ad.trace" file (i.e.,
> "C:\Users\<user>\AppData\Roaming\AnyDesk") will be created by "AnyDesk.exe"
> with "NT Authority\SYSTEM" privilege.
> [image: image.png]
> [image: image.png]
> *Affected function B*

> After a connection was made, local or remote user could use the chat room. The chat log was written to folder "C:\Users\<user>\AppData\Roaming\AnyDesk\chat\" by "AnyDesk.exe" with "NT Authority\SYSTEM" privilege. Or the local user (without admin privilege) could change the location of the chat log to anywhere that he/she has "Modify" privilege.
> [image: image.png]
> [image: image.png]
> *Vulnerability Summary*
> Since the directories (i.e., "C:\Users\<user>\AppData\Roaming\AnyDesk\", "C:\Users\<user>\AppData\Roaming\AnyDesk\chat\") were assigned with "Modify" privilege for current user, current user could modify the entire directory. With this setup, an unprivileged user is able to achieve arbitrary file write by creating a symbolic link to a privileged location (e.g., C:\Windows\System32). As a result, a malicious user could potentially deny any service by overwriting the configuration or system file of applications such as Anti Virus solutions. It was noted that the file content could be manipulated in affected function B such that a low privileged user could write an arbitrary file to an arbitrary location.
> [image: d98609c1-7ec9-4a1d-9a6c-f4ef670e5d23.png]
> *Affected function A: Exploit steps by local user (without admin privilege)*
>
> 1. Remove the directory "C:\Users\<user>\AppData\Roaming\AnyDesk"
> 2. Create symbolic link of "ad.trace" file to a privileged location (e.g., C:\Windows\System32\test.file) (PoC binary could be found here: https://github.com/googleprojectzero/symboliclink-testing-tools/blob/main/CreateSymlink/CreateSymlink_readme.txt)
>
> [image: image.png]
>
> 1. Connect to local machine (target machine) from a remote machine. After the connection was initiated, the content of "ad.trace" file would be written to target file (e.g., C:\Windows\System32\test.file)
>
> [image: image.png]
> *Affected function B: Exploit steps by local user (without admin privilege)*
>
> 1. edit username of remote connector
>
> [image: image.png]
>
> 1. Establish a AnyDesk connection from remote. Enter arbitrary text into the chat box. Mark down the filename of chat log
>
> [image: image.png]
>
> 1. Remove the directory "C:\Users\<user>\AppData\Roaming\AnyDesk\chat"
> 2. Create symbolic link of chat log file (e.g., 657584961.txt) to a privileged location (e.g., C:\Windows\test.conf) (PoC binary could be found here: https://github.com/googleprojectzero/symboliclink-testing-tools/blob/main/CreateSymlink/CreateSymlink_readme.txt)
>
> [image: image.png]
>
> 1. Open the chat room and enter arbitrary content into it. After that, the content of chat room would be written to target file (e.g., C:\Windows\test.conf)
>
> [image: image.png]
> [image: image.png]

> ```
> Please let me know if any detail need further. Thanks
>
> Regards,
> Erwin
> ```



Disconnected from the AnyDesk network.

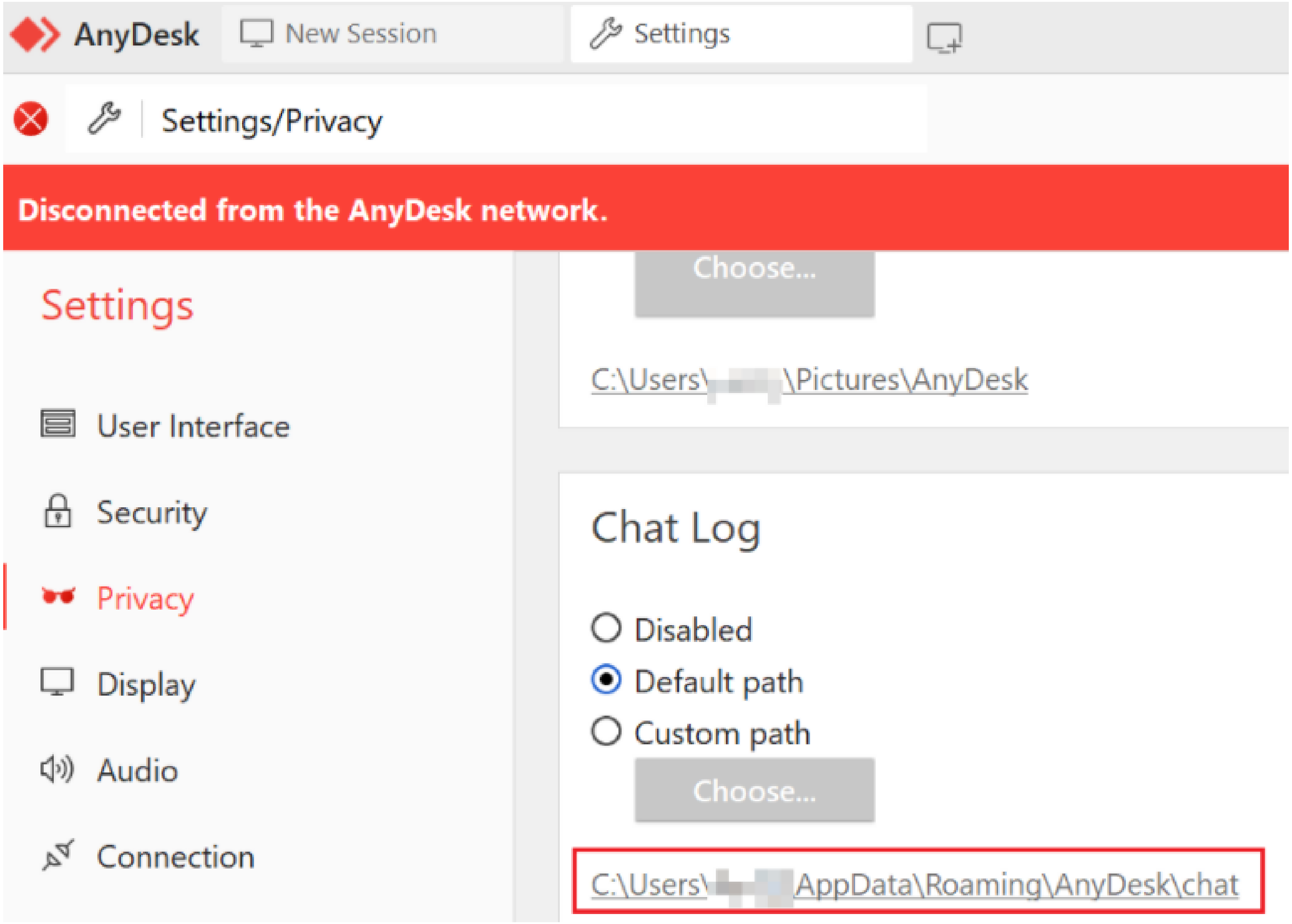
C:\Users\[redacted]\Pictures\AnyDesk

Chat Log

○ Disabled
● Default path
○ Custom path

Choose...

C:\Users\[redacted]AppData\Roaming\AnyDesk\chat



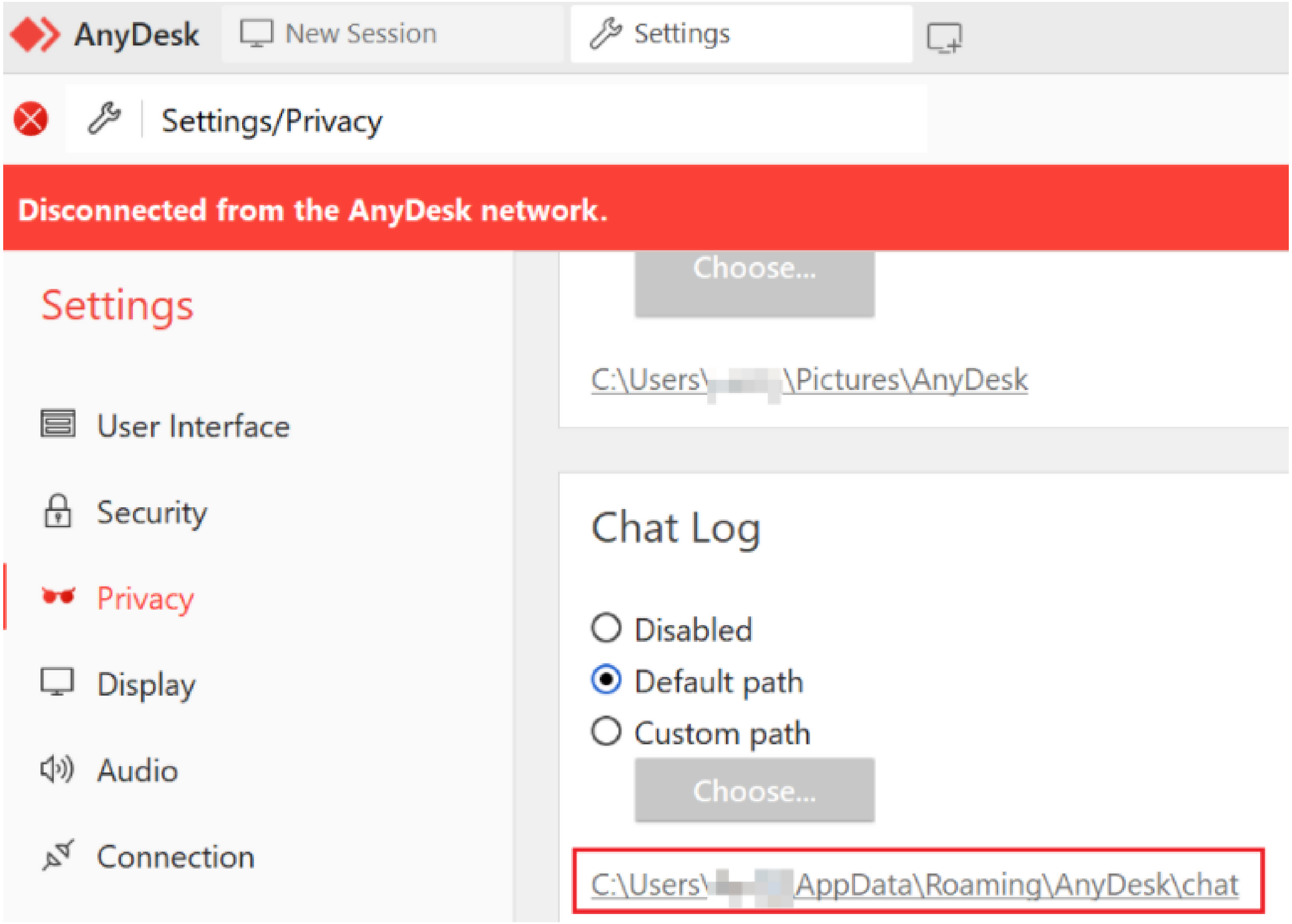
Disconnected from the AnyDesk network.

C:\Users\[redacted]\Pictures\AnyDesk

Chat Log

○ Disabled
● Default path
○ Custom path

C:\Users\[redacted]AppData\Roaming\AnyDesk\chat



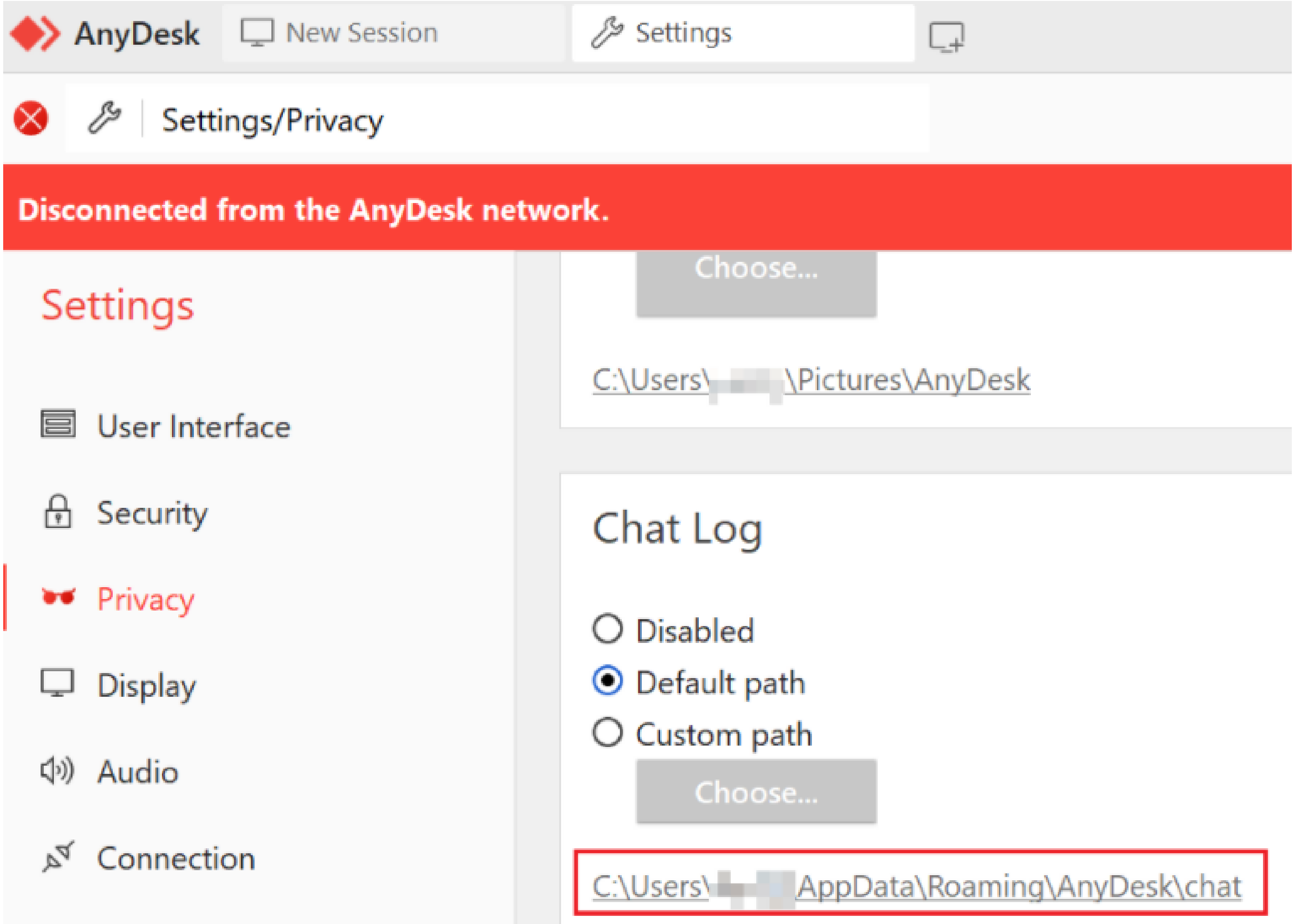
Disconnected from the AnyDesk network.

C:\Users\[redacted]\Pictures\AnyDesk

Chat Log

○ Disabled
● Default path
○ Custom path

C:\Users\[redacted]AppData\Roaming\AnyDesk\chat



Settings/Privacy

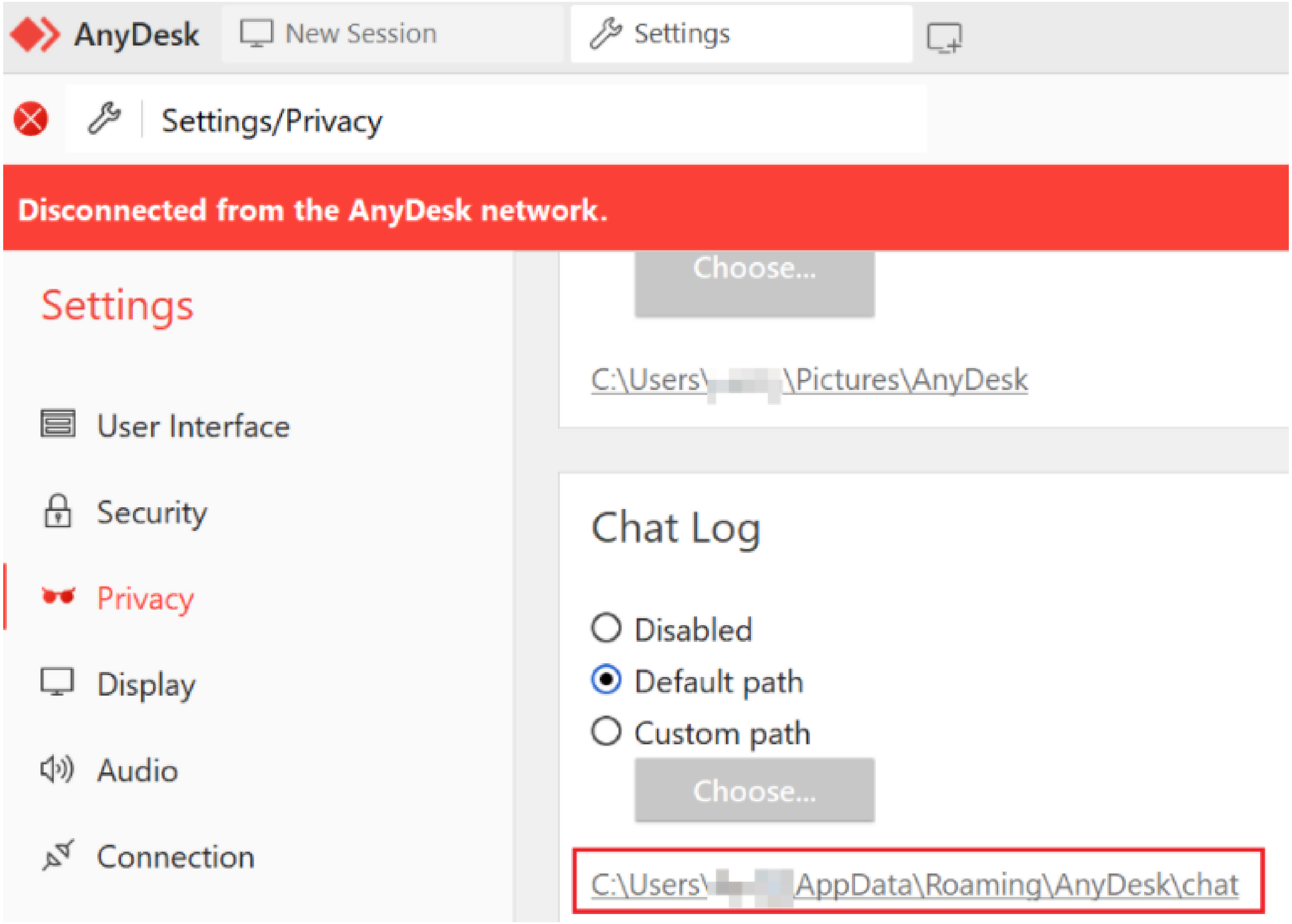
Disconnected from the AnyDesk network.

C:\Users\[redacted]\Pictures\AnyDesk

Chat Log

○ Disabled
● Default path
○ Custom path

C:\Users\[redacted]AppData\Roaming\AnyDesk\chat



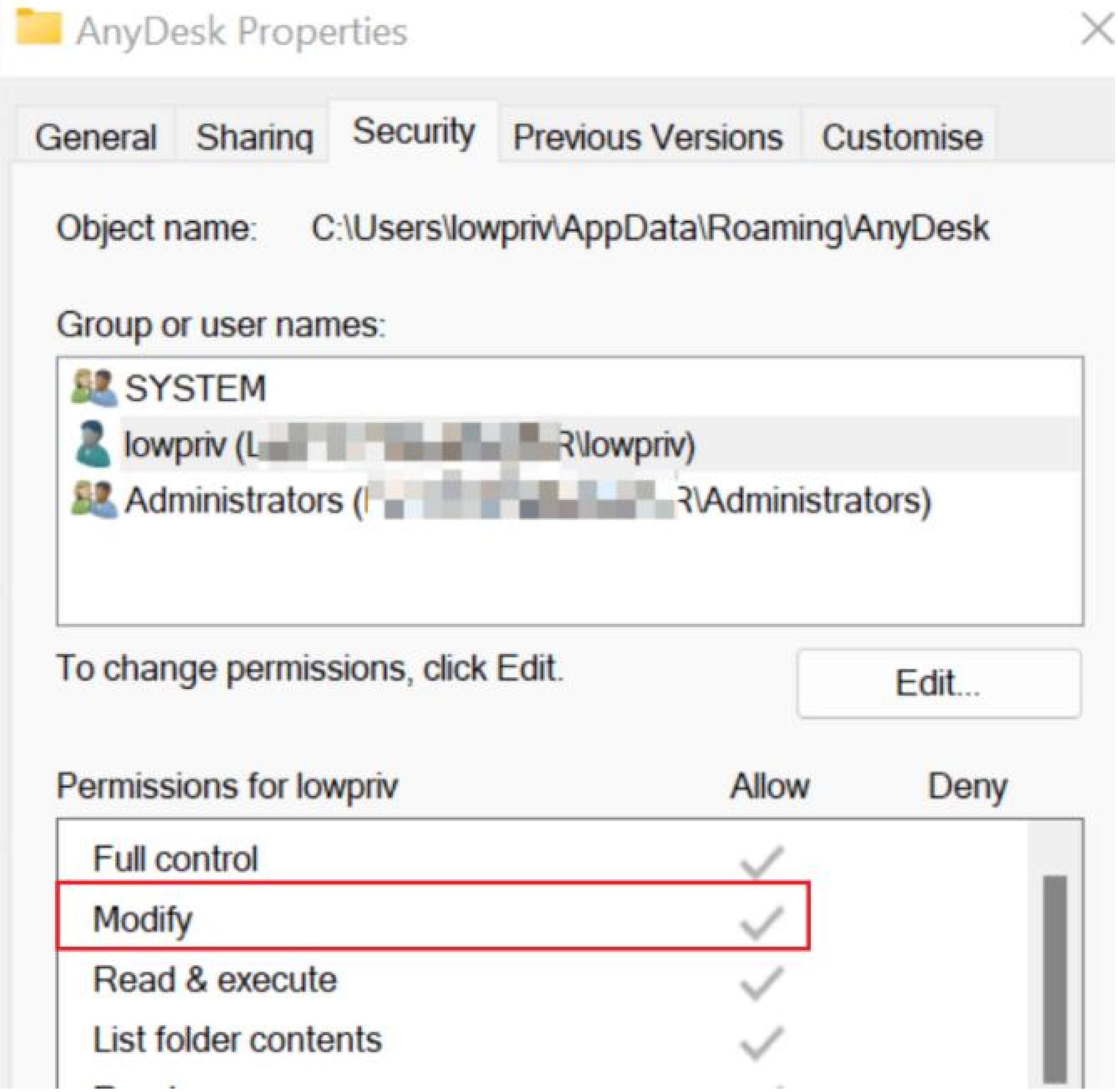
Disconnected from the AnyDesk network.

C:\Users\[redacted]\Pictures\AnyDesk

Chat Log

○ Disabled
● Default path
○ Custom path

C:\Users\[redacted]AppData\Roaming\AnyDesk\chat



Object name: C:\Users\lowpriv\AppData\Roaming\AnyDesk

Group or user names:

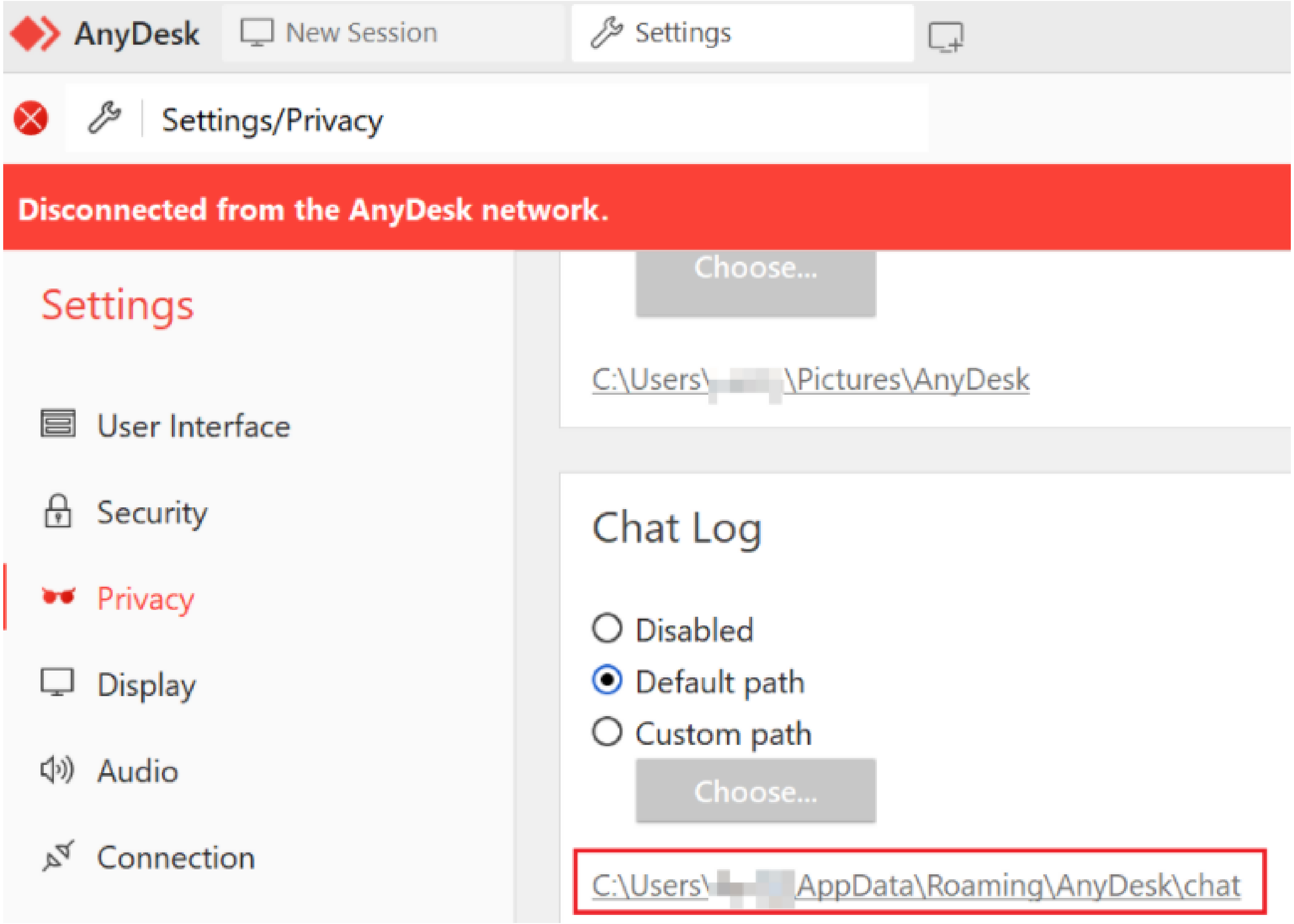
SYSTEM

lowpriv ([redacted]\lowpriv)

Administrators ([redacted]\Administrators)

To change permissions, click Edit.

Permissions for lowpriv	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	



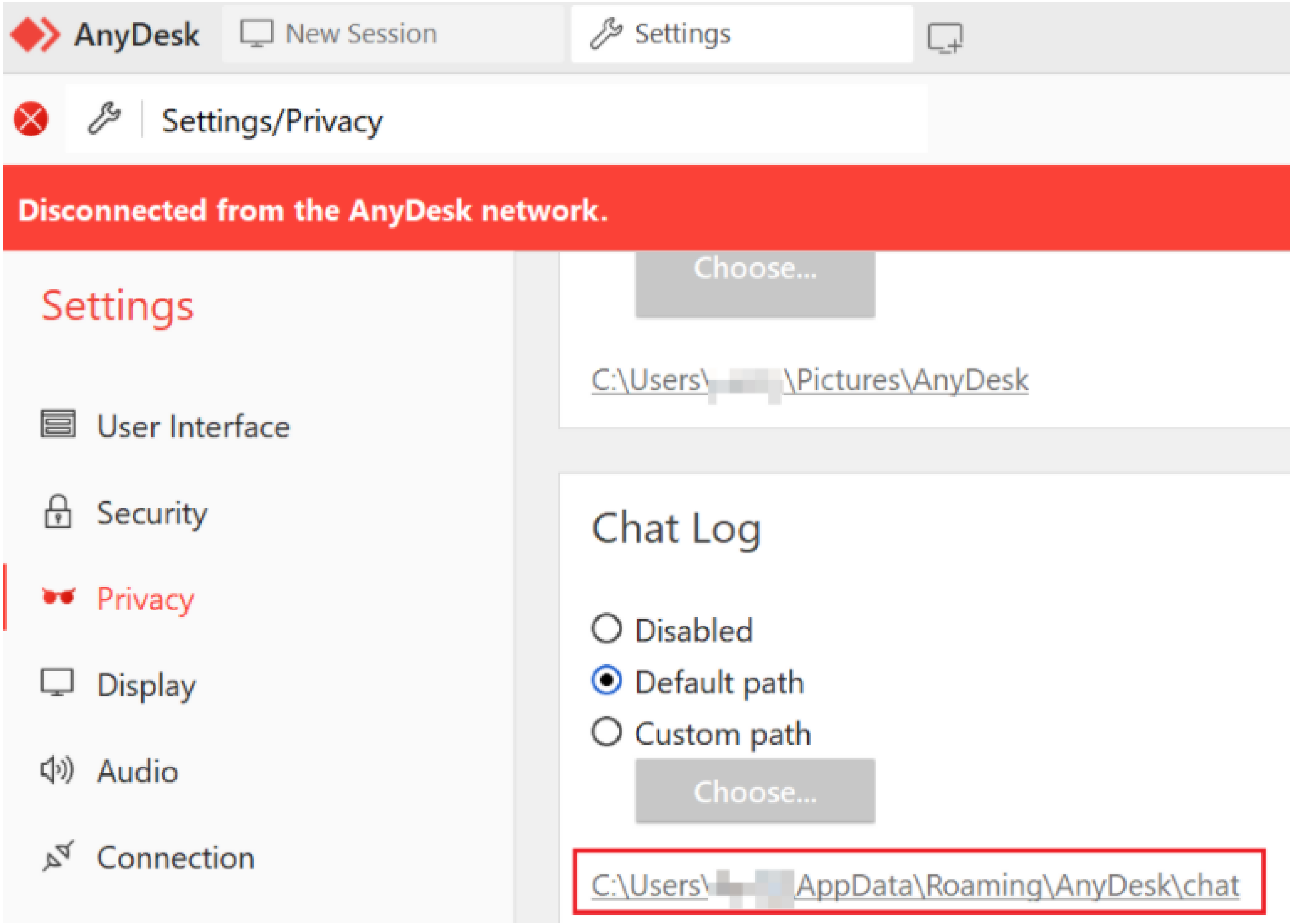
Disconnected from the AnyDesk network.

C:\Users\[redacted]\Pictures\AnyDesk

Chat Log

○ Disabled
● Default path
○ Custom path

C:\Users\[redacted]AppData\Roaming\AnyDesk\chat



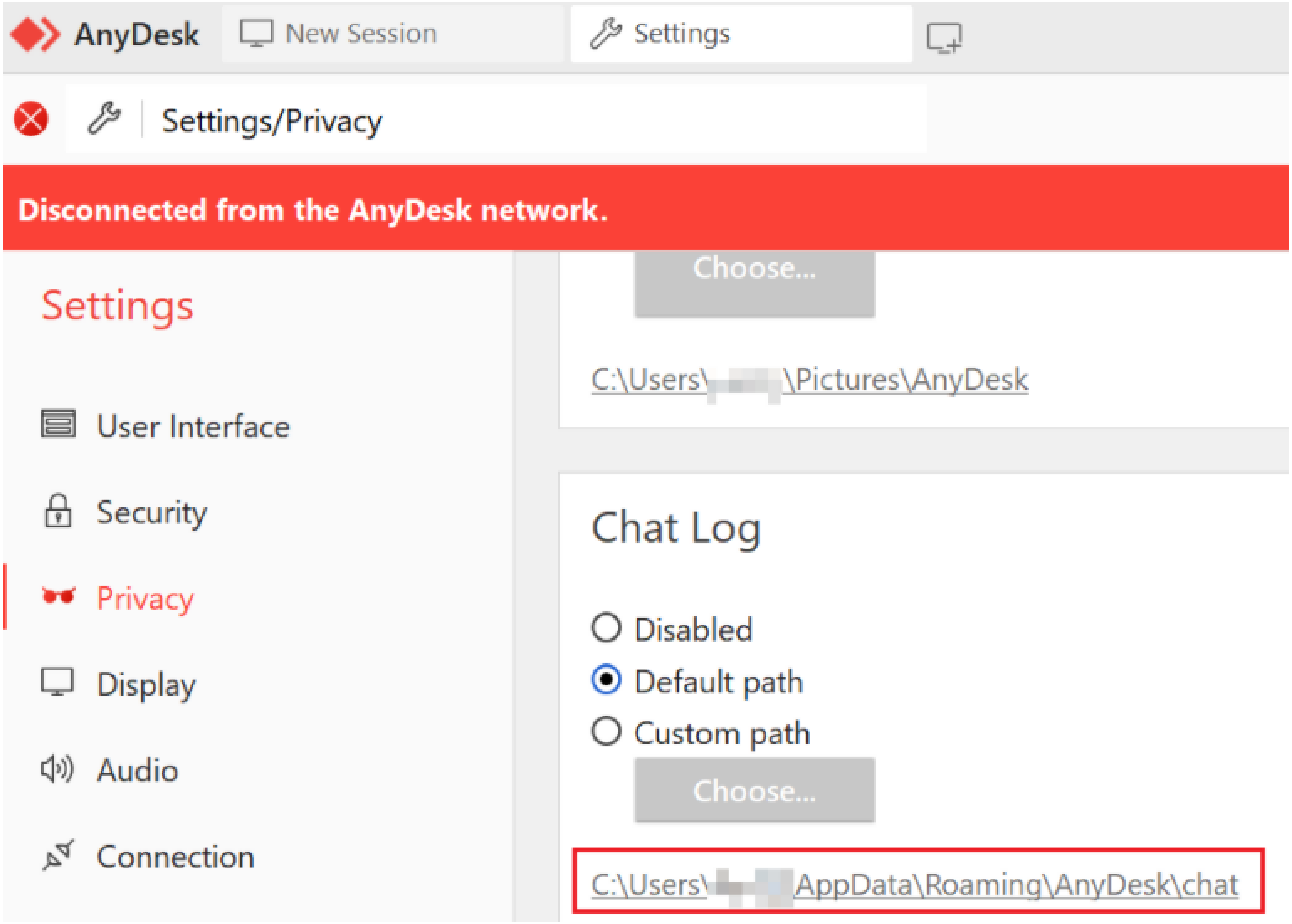
Disconnected from the AnyDesk network.

C:\Users\[redacted]\Pictures\AnyDesk

Chat Log

○ Disabled
● Default path
○ Custom path

C:\Users\[redacted]AppData\Roaming\AnyDesk\chat



Disconnected from the AnyDesk network.

C:\Users\[redacted]\Pictures\AnyDesk

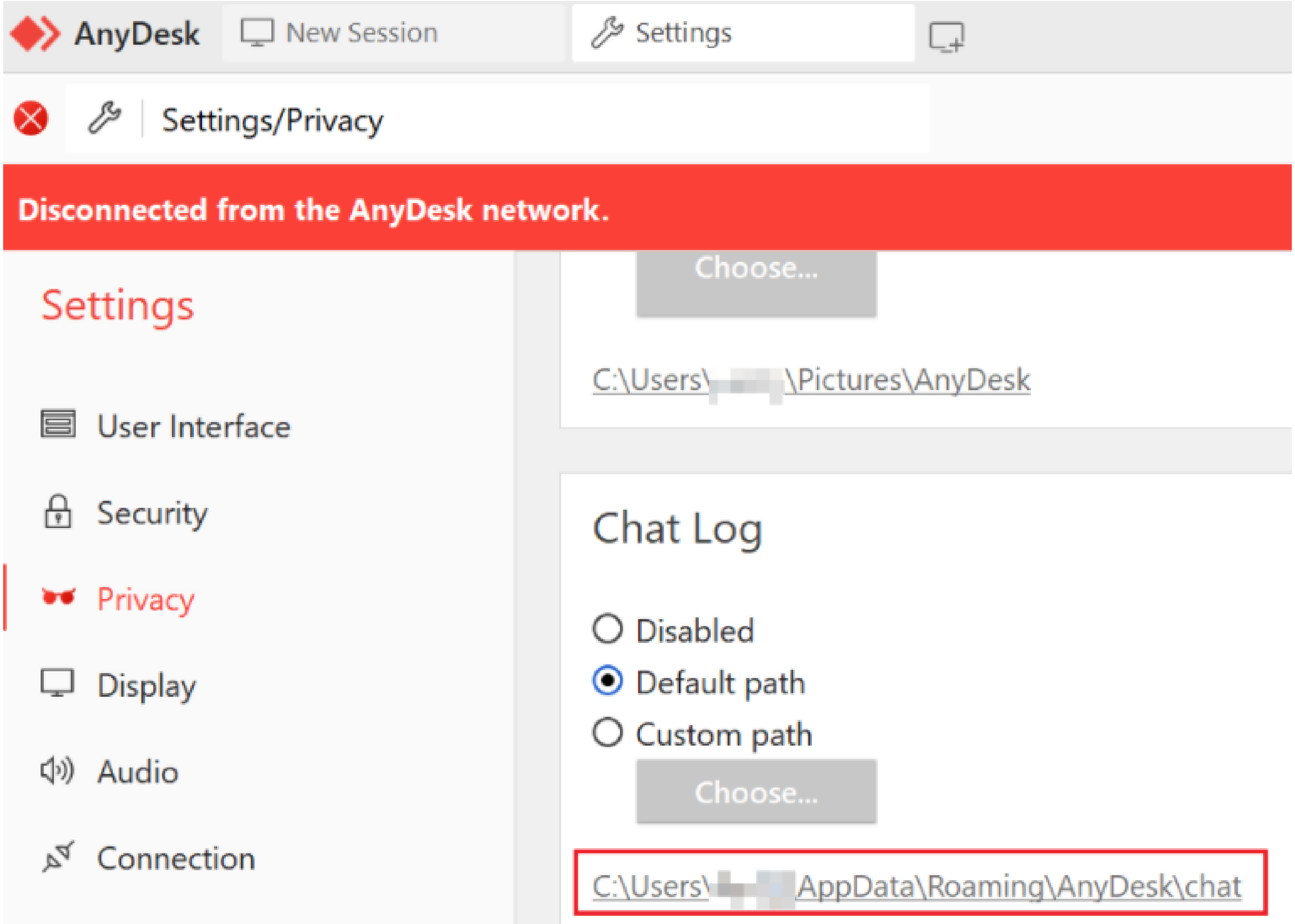
Chat Log

○ Disabled

● Default path

○ Custom path

C:\Users\[redacted]AppData\Roaming\AnyDesk\chat



Disconnected from the AnyDesk network.

C:\Users\[redacted]\Pictures\AnyDesk

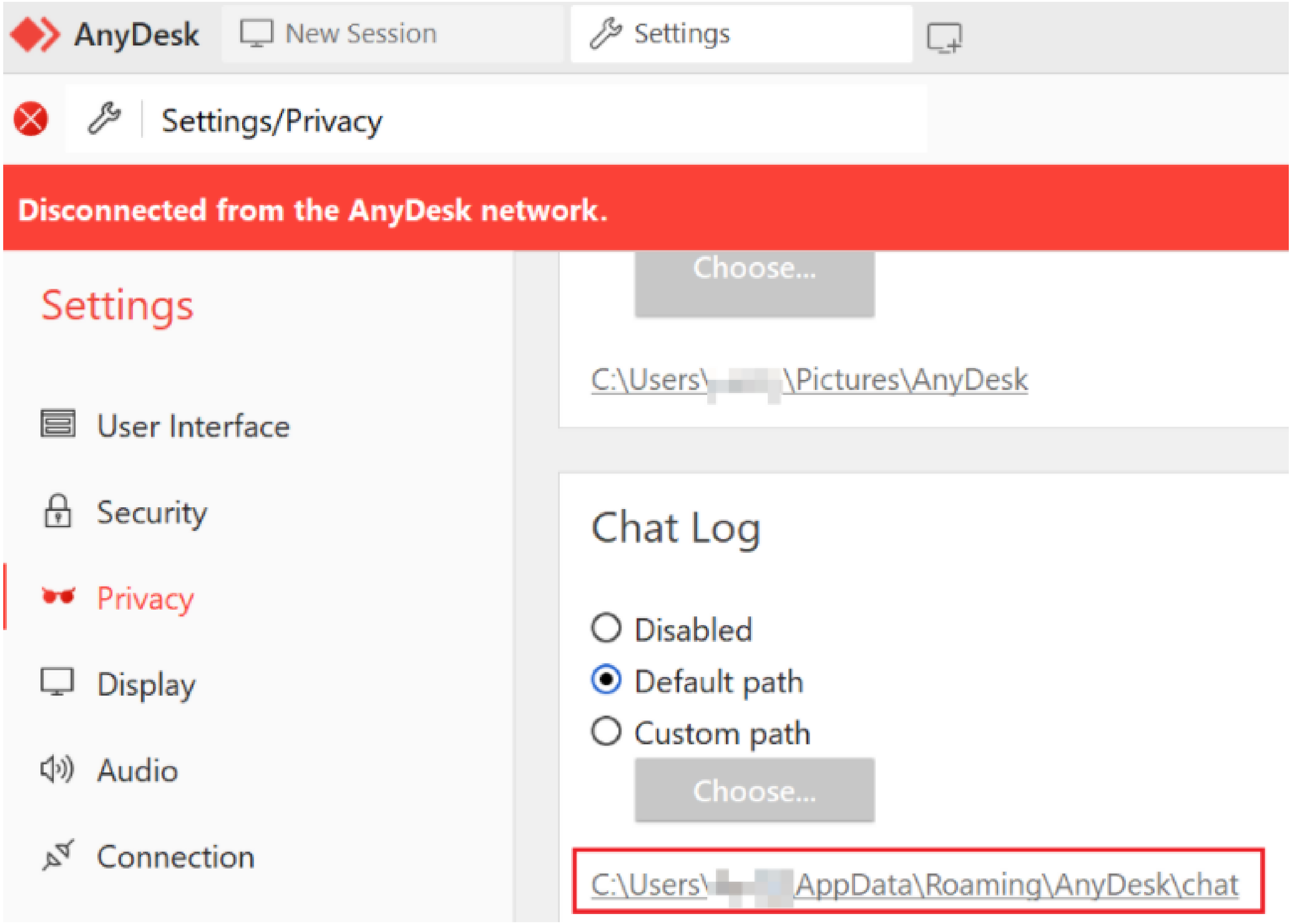
Chat Log

○ Disabled

● Default path

○ Custom path

C:\Users\[redacted]AppData\Roaming\AnyDesk\chat



Disconnected from the AnyDesk network.

C:\Users\[redacted]\Pictures\AnyDesk

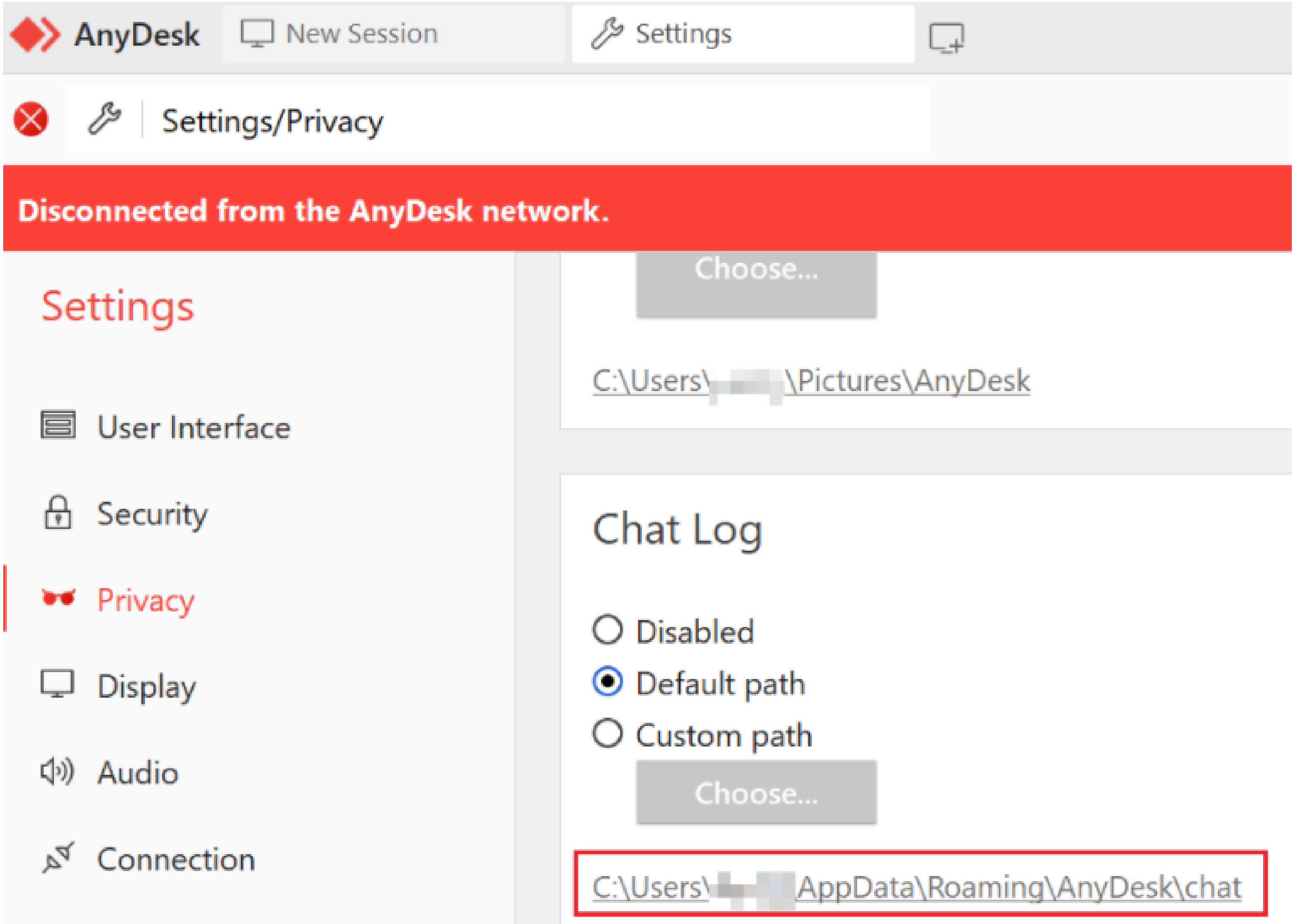
Chat Log

○ Disabled

● Default path

○ Custom path

C:\Users\[redacted]AppData\Roaming\AnyDesk\chat



Settings/Privacy

Disconnected from the AnyDesk network.

C:\Users\[redacted]\Pictures\AnyDesk

Chat Log

○ Disabled
● Default path
○ Custom path

C:\Users\[redacted]AppData\Roaming\AnyDesk\chat

```
_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: https://seclists.org/fulldisclosure/
```

By Date By Thread

Current thread:

Re: AnyDesk Public Exploit Disclosure - Arbitrary file write by symbolic link attack lead to denial-of-service attack on local machine ***chan chan (Jul 18)***

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License

Nmap OEM