

## AnyDesk 7.0.9 Arbitrary File Write / Denial Of Service

Authored by [Erwin Chan](#)

Posted Jun 28, 2022

AnyDesk version 7.0.9 suffers from an arbitrary file write vulnerability via a symlink attack.

tags | [exploit](#), [arbitrary](#)

advisories | [CVE-2022-32450](#)

SHA-256 | a24a864d0cf210e9aa4cf317353b4651dcf88793c38af3fcf86fc7d93525574a [Download](#) | [Favorite](#) | [View](#)

### Related Files

### Share This

Like 0

Tweet

LinkedIn

Reddit

Digg

StumbleUpon

### Change Mirror

[Download](#)

```
# 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.

#### \*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.

#### \*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.

#### \*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
)
```

```
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)
```

#### \*Affected function B: Exploit steps by local user (without admin privilege)\*

```
1. edit username of remote connector
```

```
1. Establish a AnyDesk connection from remote. Enter arbitrary text into
the chat box. Mark down the filename of chat log
```

```
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
)
```



Follow us on Twitter



Subscribe to an RSS Feed

### File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

### Top Authors In Last 30 Days

**Red Hat** 188 files

**Ubuntu** 57 files

**Gentoo** 44 files

**Debian** 28 files

**Apple** 25 files

**Google Security Research** 14 files

**malvuln** 10 files

**nu11secu1ty** 6 files

**mjrczyk** 4 files

**George Tsimpidas** 3 files

### File Tags

ActiveX (932)

Advisory (79,557)

Arbitrary (15,643)

BBS (2,859)

Bypass (1,615)

CGI (1,015)

Code Execution (6,913)

Conference (672)

Cracker (840)

CSRF (3,288)

DoS (22,541)

Encryption (2,349)

Exploit (50,293)

File Inclusion (4,162)

File Upload (946)

Firewall (821)

Info Disclosure (2,656)

### File Archives

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

December 2021

Older

### Systems

AIX (426)

Apple (1,926)

```
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)
```

Please let me know if any detail need further. Thanks

Regards,  
Erwin

[Login](#) or [Register](#) to add favorites

<a href="#">Intrusion Detection (866)</a>	<a href="#">BSD (370)</a>
<a href="#">Java (2,888)</a>	<a href="#">CentOS (55)</a>
<a href="#">JavaScript (817)</a>	<a href="#">Cisco (1,917)</a>
<a href="#">Kernel (6,255)</a>	<a href="#">Debian (6,620)</a>
<a href="#">Local (14,173)</a>	<a href="#">Fedora (1,690)</a>
<a href="#">Magazine (586)</a>	<a href="#">FreeBSD (1,242)</a>
<a href="#">Overflow (12,390)</a>	<a href="#">Gentoo (4,272)</a>
<a href="#">Perl (1,417)</a>	<a href="#">HPUX (878)</a>
<a href="#">PHP (5,087)</a>	<a href="#">iOS (330)</a>
<a href="#">Proof of Concept (2,290)</a>	<a href="#">iPhone (108)</a>
<a href="#">Protocol (3,426)</a>	<a href="#">IRIX (220)</a>
<a href="#">Python (1,449)</a>	<a href="#">Juniper (67)</a>
<a href="#">Remote (30,009)</a>	<a href="#">Linux (44,118)</a>
<a href="#">Root (3,496)</a>	<a href="#">Mac OS X (684)</a>
<a href="#">Ruby (594)</a>	<a href="#">Mandriva (3,105)</a>
<a href="#">Scanner (1,631)</a>	<a href="#">NetBSD (255)</a>
<a href="#">Security Tool (7,768)</a>	<a href="#">OpenBSD (479)</a>
<a href="#">Shell (3,098)</a>	<a href="#">RedHat (12,339)</a>
<a href="#">Shellcode (1,204)</a>	<a href="#">Slackware (941)</a>
<a href="#">Sniffer (885)</a>	<a href="#">Solaris (1,607)</a>
<a href="#">Spoof (2,165)</a>	<a href="#">SUSE (1,444)</a>
<a href="#">SQL Injection (16,089)</a>	<a href="#">Ubuntu (8,147)</a>
<a href="#">TCP (2,377)</a>	<a href="#">UNIX (9,150)</a>
<a href="#">Trojan (685)</a>	<a href="#">UnixWare (185)</a>
<a href="#">UDP (875)</a>	<a href="#">Windows (6,504)</a>
<a href="#">Virus (661)</a>	<a href="#">Other</a>
<a href="#">Vulnerability (31,104)</a>	
<a href="#">Web (9,329)</a>	
<a href="#">Whitepaper (3,728)</a>	
<a href="#">x86 (946)</a>	
<a href="#">XSS (17,478)</a>	
<a href="#">Other</a>	

**packet storm**  
© 2022 Packet Storm. All rights reserved.

## Site Links

[News by Month](#)

[News Tags](#)

[Files by Month](#)

[File Tags](#)

[File Directory](#)

## About Us

[History & Purpose](#)

[Contact Information](#)


[Terms of Service](#)


[Privacy Statement](#)

[Copyright Information](#)

## Hosting By

[Rokasec](#)

 [Follow us on Twitter](#)

 [Subscribe to an RSS Feed](#)