CVE-2022-32450

Published on: Not Yet Published

Last Modified on: 07/22/2022 02:33:00 PM UTC

CVE-2022-32450

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF

Certain versions of Anydesk from Anydesk contain the following vulnerability:

AnyDesk 7.0.9 allows a local user to gain SYSTEM privileges via a symbolic link because the user can write to their own %APPDATA% folder (used for ad.trace and chat) but the product runs as SYSTEM when writing chat-room data there.

CVE-2022-32450 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	HIGH

CVE References

Description	Tags	Link
Full Disclosure: Re: AnyDesk Public Exploit Disclosure - Arbitrary file write by symbolic link attack lead to denial-of-service attack on local machine	seclists.org text/html	FULLDISC 20220718 Re: AnyDesk Public Exploit Disclosure - Arbitrary file write by symbolic link attack lead to denial-of-service attack on local machine
AnyDesk 7.0.9 Arbitrary File Write / Denial Of Service ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/167608/AnyDesk-7.0.9-Arbitrary-File-Write-Denial-Of-Service.html
The Fast Remote Desktop Application – AnyDesk	anydesk.com text/html	MISC anydesk.com
Full Disclosure: AnyDesk Public Exploit Disclosure - Arbitrary file write by symbolic link attack lead to denial-of-service attack on local machine	seclists.org text/html	MISC seclists.org/fulldisclosure/2022/Jun/44

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Anydesk	Anydesk	7.0.9	All	All	All

cpe:2.3:a:anydesk:anydesk:7.0.9:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-32450 : AnyDesk 7.0.9 allows a local user to gain SYSTEM privileges via a symbolic link because the user c… twitter.com/i/web/status/1…	2022-07-18 13:08:08
/r/netcve	CVE-2022-32450	2022-07-18 14:39:02

← Previous ID

Next ID→