مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Escalation Vulnerability in AnyDesk

Tracking #:432316846

Date:10-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in AnyDesk that could be exploited to gain full control of affected systems.

TECHNICAL DETAILS:

A security vulnerability (CVE-2024-12754) exist in AnyDesk, a widely used remote administration software. This flaw enables local privilege escalation, allowing a low-privileged user to gain elevated access and potentially take full control of a system.

Vulnerability Details:

- **CVE-2024-12754**
- CVSS Base Score: 5.5 MEDIUM
- The vulnerability arises from an arbitrary file read/copy operation executed by the AnyDesk service running under **NT AUTHORITY\SYSTEM** privileges. Specifically, the flaw allows a low-privileged user to manipulate the way AnyDesk handles background images, enabling them to:
  - Set their own background image, which AnyDesk then copies to C:\Windows\Temp.
  - Pre-create a file with the same name in C:\Windows\Temp.
  - Exploit the fact that AnyDesk overwrites the existing file while retaining SYSTEM-level ownership and permissions.
- By leveraging this flaw, an attacker can gain control over sensitive system files such as **SAM, SYSTEM, and SECURITY**, leading to credential extraction and full system compromise.
- A Proof-of-Concept PoC exploit for CVE-2024-12754 is publicly available. Increasing the risk of exploitation.

Affected Versions:

- AnyDesk (prior to v9.0.1)

Fixed Version:

- AnyDesk v9.0.1 or later

RECOMMENDATIONS:

- Ensure AnyDesk is updated to the latest or fixed version
- **Restrict Access**:
  1. Limit permissions for low-privileged users on directories like C:\Windows\Temp.
  2. Monitor and secure access to sensitive files and directories.
- **Disable Volume Shadow Copies**: If not required, disabling Volume Shadow Copies can reduce the risk of attackers accessing backup files like SAM or SYSTEM.
- **Monitor Abnormal Activity**: Implement tools to detect unusual file operations or junction manipulations.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2024-12754
- https://mansk1es.gitbook.io/AnyDesk_CVE-2024-12754
- https://github.com/CICADA8-Research/Penetration/tree/main/POCs/CVE-2024-12754