مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Zero-Day Vulnerability in AnyDesk

Tracking #:432316547

Date:22-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a zero-day vulnerability in AnyDesk that could potentially be exploited by attackers to obtain sensitive IP address information from target systems.

TECHNICAL DETAILS:

A zero-day vulnerability (CVE-2024-52940) exists in AnyDesk, a popular remote desktop software, affecting versions 8.1.0 and below on Windows systems. This flaw in the "Allow Direct Connections" feature can expose users' public IP addresses, posing significant privacy and security risk

Vulnerability Details:

- **CVE-2024-52940**
- CVSS v3.1 Base Score: 7.5 (High)
- The vulnerability stems from the “Allow Direct Connections” feature in AnyDesk, which, when enabled, can expose the public IP address of a target system to an attacker. In certain scenarios, the attacker may also be able to obtain the private IP address.
- When the "Allow Direct Connections" feature is enabled and the connection port is set to 7070 on the attacker's system, an attacker can retrieve the public IP address of a target using only their AnyDesk ID. This requires no configuration changes on the victim's system.
- Exploitation of this vulnerability can lead to:
  - Exposure of users' public IP addresses
  - Potential exposure of private IP addresses within the same network
  - Increased risk of targeted attacks, including phishing and DoS
  - Possible compromise of user location privacy
- A proof of concept (PoC) for CVE-2024-52940 publicly available.

Affected Versions:

- AnyDesk 8.1.0 and below on Windows

RECOMMENDATIONS:

- Disable the "Allow Direct Connections" feature until a patch is released.
- Exercise caution when using AnyDesk, especially in sensitive environments.
- Monitor for updates from AnyDesk and apply them promptly when available.
- Monitor for unusual network traffic related to AnyDesk connections
- Consider temporarily blocking AnyDesk in high-security environments

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-2024-52940