مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Aviatrix Controller

Tracking #:432316715

Date:08-01-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the Aviatrix Network Controller that could allow attackers to execute malicious code on affected systems.

TECHNICAL DETAILS:

A critical command injection vulnerability (CVE-2024-50603) exists in Aviatrix Network Controller. This vulnerability allows unauthenticated attackers to execute arbitrary code remotely, posing severe risks to enterprises using Aviatrix for cloud networking solutions.

Vulnerability Details:

- CVE-2024-50603
- CVSS Score: 10.0 (Critical)
- The vulnerability stems from improper neutralization of special elements in system commands within the Aviatrix Controller's API. Specifically, the cloud_type parameter in the list_flightpath_destination_instances action is not properly sanitized, allowing command injection.
- Successful exploitation of this vulnerability could result in:
  - Remote Code Execution with system-level privileges.
  - Data Exfiltration of sensitive system files and information.
  - Full System Compromise, enabling lateral movement and further exploitation.

Affected Versions:

- Aviatrix Controller versions 7.x through 7.2.4820

Fixed Versions:

- Aviatrix Controller to version 7.2.4996 or later

RECOMMENDATIONS:

- **Update Immediately:** Upgrade the Aviatrix Controller to the latest version.
- **Restrict Access:** Limit network exposure of the Aviatrix Controller to trusted IP addresses.
- **Monitor Logs:** Review server and network logs for signs of exploitation.

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-2024-50603