



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Increase in Cyber threat activity targeting Snowflake Customer Accounts**

Tracking #:432315921

Date:04-06-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed increase in cyber threat activity targeting Snowflake customer accounts that caused successful compromises of several companies utilising Snowflake environments.

## TECHNICAL DETAILS:

A recent increase in cyber threat activity targeting Snowflake customer accounts has observed and the attacks leverage stolen credentials, obtained from unrelated breaches, to gain unauthorized access to customer data. While Snowflake itself is not believed to be vulnerable, compromised user credentials pose a significant risk.

- Review user access: Immediately review all user accounts and access controls within your Snowflake environment. Identify and remove any unused or unnecessary accounts.
- Implement strong password policies: Enforce strong password policies including minimum length, complexity requirements, and regular password rotation. Consider multi-factor authentication (MFA) for an additional layer of security.
- Monitor for suspicious activity: Enable activity monitoring within Snowflake to identify any unusual login attempts or data access patterns.
- Educate users: Educate your users on best practices for password hygiene and cybersecurity awareness. Train them to identify and report suspicious phishing attempts.

### Mitigations:

- Snowflake have published an [advisory](#) to assist in identifying instances of unauthorized access.

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to review the snowflake advisory and implement mitigations.

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://community.snowflake.com/s/article/Communication-ID-0108977-Additional-Information>