TWILIO DATA BREACH

Nadja Cizmic

ABOUT TWILIO

WHO ARE THEY ?

Twilio is an American company, with headquarters in San Francisco, California. They offer programmable communication tools for sending and receiving text messages, making and receiving phone calls, and carrying out other communication tasks through its web service APIs.

TWILIO DATA BREACH

On August 4, 2022, Twilio became aware of unauthorized access to information related to a limited number of Twilio customer accounts through a sophisticated social engineering attack designed to steal employee credentials. This broad based attack against their employee base succeeded in fooling some employees into providing their credentials. The attackers then used the stolen credentials to gain access to some of their internal systems, where they were able to access certain customer data.

Current and former employees reported receiving text messages from IT department. Text bodies suggested that the employee's passwords had expired, or that their schedule had changed, and that they needed to log in to a URL the attacker controls. The URLs used words including "Twilio," "Okta," and "SSO" to try and trick users to click on a link taking them to a landing page that impersonated Twilio’s sign-in page.

WHAT WAS AFFECTED

- 209 customers out of a total customer base of over 270,000 and 93 Authy end users out of approximately 75 million total users had accounts that were impacted by the incident;
- There was no evidence that the malicious actors accessed Twilio customers’ console account credentials, authentication tokens, or API keys.

ACTIONS THEY TOOK TO EREDICATE MALICIOUS ACCESS

- Resetting credentials of the compromised Twilio employee user accounts;
- Revoking all active sessions associated with the compromise of Okta-integrated apps;
- Blocking all indicators of compromise associated with the attack;
- Initiating takedown requests of the fake Twilio domains.

THEIR PLAN TO PREVENT FUTURE DATA BREACHES

- Implementing stronger two factor precautions and distributing FIDO2 tokens to all employees;
- Implementing additional layers of control within their VPN;
- Removing and limiting certain functionality within specific administrative tooling;
- Increasing the refresh frequency of tokens for Okta-integrated applications;
- Conducting supplemental mandatory security training for all employees regarding attacks based on social engineering techniques.

THANK YOU