مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Twilio Authy Information Disclosure Vulnerability

Tracking #:432316085

Date:24-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that an unsecured API endpoint allowed threat actors to access and verify the phone numbers of millions of users of the Authy multi-factor authentication (MFA) app.

TECHNICAL DETAILS:

It was discovered that an unsecured API endpoint allowed threat actors to access and verify the phone numbers of millions of users of the Authy multi-factor authentication (MFA) app. ShinyHunters, a known hacker group, leaked a CSV file containing over 33 million phone numbers, exposing users to potential SMS phishing and SIM swapping attacks. Twilio, the parent company of Authy, has since secured the endpoint and urged users to update their apps for enhanced security.

- **CVE-2024-39891-** In the Twilio Authy API, accessed by Authy Android before 25.1.0 and Authy iOS before 26.1.0, an unauthenticated endpoint provided access to certain phone-number data, as exploited in the wild.
- Updated Authy Applications Versions: Android: v25.1.0, iOS: v26.1.0

RECOMMENDATIONS:

- Update Authy Applications to the latest version.
- Enhance Account Security-Activate additional security measures offered by mobile carriers to prevent unauthorized access.
- Remain alert for potential SMS phishing attacks designed to steal sensitive information, such as passwords.
- Monitor accounts regularly for unauthorized transactions or access

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-2024-39891