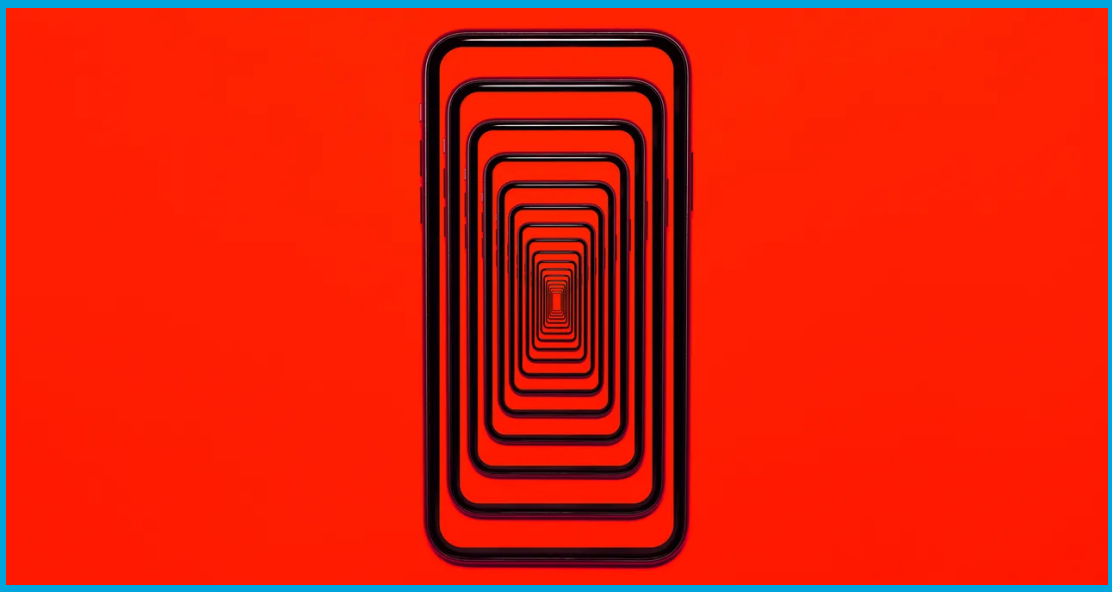
kindred

Security Newsletter

29 Aug 2022

Subscribe to this newsletter

Why the Twilio Breach Cuts So Deep



The communication company Twilio suffered a breach at the beginning of August that it says impacted 163 of its customer organizations. Out of Twilio's 270,000 clients, 0.06 percent might seem trivial, but the company's particular role in the digital ecosystem means that that fractional slice of victims had an outsized value and influence. The secure messaging app Signal, two-factor authentication app Authy, and authentication firm Okta are all Twilio customers that were secondary victims of the breach.

Twilio provides application programming interfaces through which companies can automate call and texting services. This could mean a system a barber uses to remind customers about haircuts and have them text back “Confirm” or “Cancel.” But it can also be the platform through which organizations manage their two-factor authentication text messaging systems for sending one-time authentication codes. Though it's long been known that SMS is an insecure way to receive these codes, it's definitely better than nothing, and organizations haven't been able to move away from the practice completely. Even a company like Authy, whose core product is an authentication code-generating app, uses some of Twilio's services.

Read More on Wired

More #News

- CISA: Prepare now for quantum computers, not when hackers use them
- FBI warns of residential proxies used in credential stuffing attacks
- California AG looks ahead to other data privacy violations after $1.2 million Sephora fine
- FCC launches investigation into mobile carriers' geolocation data practices
- Facebook agrees to settle class action lawsuit related to Cambridge Analytica data breach
- Security and Cheap Complexity

#Breach Log

- DoorDash discloses new data breach tied to Twilio hackers
- Twilio breach let hackers see Okta's one-time MFA passwords
- Twilio breach let hackers gain access to Authy 2FA accounts
- RansomEXX claims ransomware attack on Sea-Doo, Ski-Doo maker
- Plex warns users to reset passwords after a data breach
- French hospital hit by $10M ransomware attack, sends patients elsewhere
- Greek natural gas operator suffers ransomware-related data breach

#Patch Time!

- Atlassian Bitbucket Server vulnerable to critical RCE vulnerability
- GitLab 'strongly recommends' patching critical RCE vulnerability

#Tech and #Tools

- Crypto Miner malware disguised as Google translate desktop and other legitimate applications
- Tool Release – JWT-Reauth
- You're (Still) Doing IoT RNG
- A technical analysis of Pegasus for Android – Part 1

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us