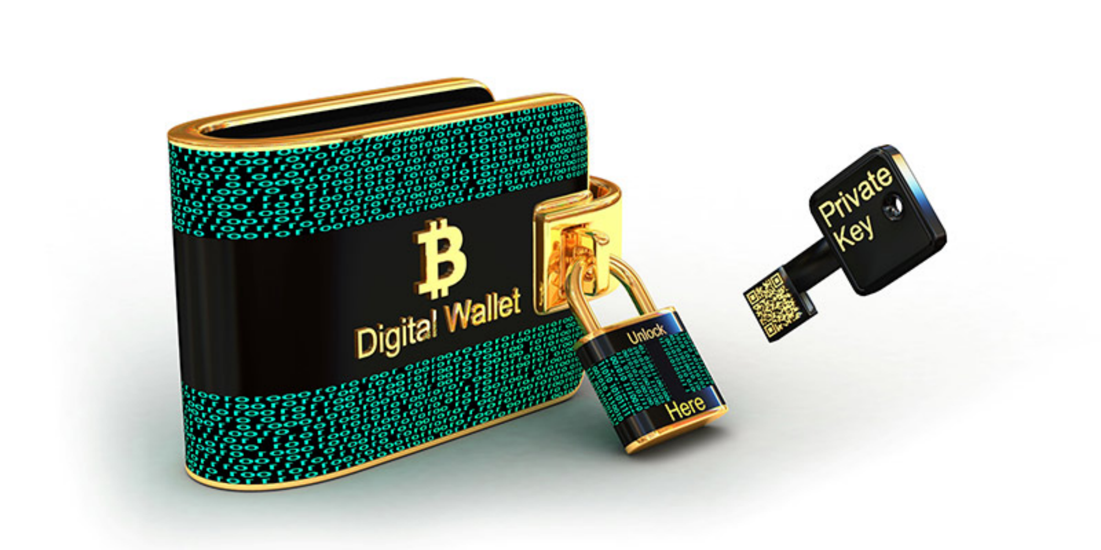
Security Newsletter

4 Oct 2021

Subscribe to this newsletter

MFA Glitch Leads to 6K+ Coinbase Customers Getting Robbed



The accounts of at least 6,000 Coinbase customers were robbed of funds after attackers bypassed the cryptocurrency exchange's multi-factor authentication (MFA).

According to a notification letter Coinbase sent to affected customers and filed with the California state Attorney General's office, the theft happened between March and May 20, 2021.

The attacker(s) used a flaw in Coinbase's account recovery process to seize the SMS two-factor authentication tokens needed to break into customers' accounts and transfer funds to crypto wallets unassociated with Coinbase.

Read More on Threatpost

Even More on ZDNet

New Azure AD Bug Lets Hackers Brute-Force Passwords Without Getting Caught

Cybersecurity researchers have disclosed an unpatched security vulnerability in the protocol used by Microsoft Azure Active Directory that potential adversaries could abuse to stage undetected brute-force attacks.

"This flaw allows threat actors to perform single-factor brute-force attacks against Azure Active Directory (Azure AD) without generating sign-in events in the targeted organization's tenant," researchers from Secureworks Counter Threat Unit (CTU) said in a report published on Wednesday.

OThe weakness resides in the Seamless Single Sign-On feature that allows employees to automatically sign when using their corporate devices that are connected to enterprise networks without having to enter any passwords.

Read More on The Hacker News

Even More on SecureWorks

More #News

- Baby's Death Alleged to Be Linked to Ransomware
- FCC Proposal Targets SIM Swapping, Port-Out Fraud
- The Rise of One-Time Password Interception Bots
- Apple 'Still Investigating' Unpatched and Public iPhone Vulnerabilities
- US unites 30 countries to disrupt global ransomware attacks
- US Congress asks FBI to explain delay in helping Kaseya attack victims

- US Congress asks FBI to explain delay in helping Kaseya attack victims
- Apple Pay with VISA lets hackers force payments on locked iPhones
- Facebook open-sources tool to find Android app security flaws
- Russia arrests cybersecurity firm CEO after raiding offices
- CISA releases tool to help orgs fend off insider threat risks
- NSA, CISA Release Guidance on Selecting and Hardening Remote Access VPNs
- Microsoft WPBT flaw lets hackers install rootkits on Windows devices
- Fortinet, Shopify and more report issues after root CA certificate from Lets Encrypt expires
- Facebook open-sources internal tool used to detect security bugs in Android apps

#Breach Log

- Sandhills online machinery markets shut down by ransomware attack
- Neiman Marcus sends notices of breach to 4.3 million customers
- JVCKenwood hit by Conti ransomware claiming theft of 1.5TB data
- Trucking giant Forward Air reports ransomware data breach
- New Android malware steals millions after infecting 10M phones

#Patch Time!

- QNAP fixes bug that let attackers run malicious commands remotely
- Google pushes emergency Chrome update to fix two zero-days
- Working exploit released for VMware vCenter CVE-2021-22005 bug
- The discovery of Gatekeeper bypass CVE-2021-1810

#Tech and #Tools

- Free Tool to Discover Unprotected Cloud Storage Instances
- PixStealer: a new wave of Android banking Trojans abusing Accessibility Services
- New Version Of Apostle Ransomware Reemerges In Targeted Attack On Higher Education
- An Intro to Fuzzing (AKA Fuzz Testing)
- Exploiting Client-Side Prototype Pollution in the wild
- Cisco Hyperflex: How We Got RCE Through Login Form and Other Findings
- GitOops! Lateral movement and privesc in GitHub orgs via CI/CD pipelines
- fail2ban – Remote Code Execution

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 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 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