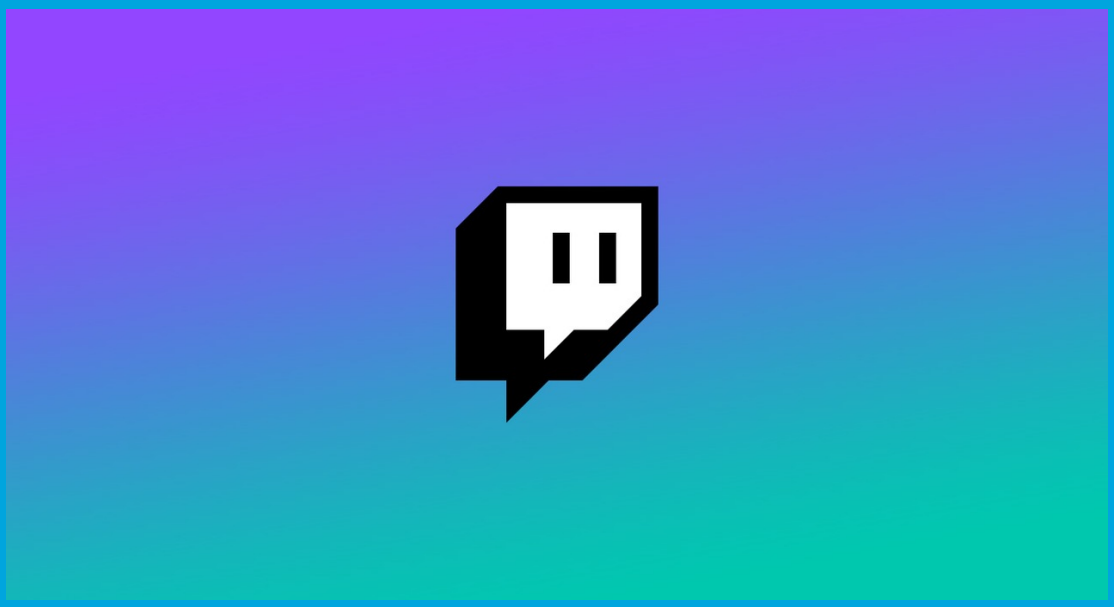
kindred

Security Newsletter

11 Oct 2021

Subscribe to this newsletter

Twitch Suffers Massive Data Leak Due to Server Misconfiguration



Interactive livestreaming platform Twitch acknowledged a "breach" after an anonymous poster on the 4chan messaging board leaked its source code, an unreleased Steam competitor from Amazon Game Studios, details of creator payouts, proprietary software development kits, and other internal tools.

The Amazon-owned service said it's "working with urgency to understand the extent of this," adding the data was exposed "due to an error in a Twitch server configuration change that was subsequently accessed by a malicious third party."

"At this time, we have no indication that login credentials have been exposed," Twitch noted in a post published late Wednesday. "Additionally, full credit card numbers are not stored by Twitch, so full credit card numbers were not exposed."

Read More on The Hacker News

Even More on Twitch blog

Company That Routes Billions of Text Messages Quietly Says It Was Hacked

A company that is a critical part of the global telecommunications infrastructure used by AT&T, T-Mobile, Verizon and several others around the world such as Vodafone and China Mobile, quietly disclosed that hackers were inside its systems for years, impacting more than 200 of its clients and potentially millions of cellphone users worldwide.

The company, Syniverse, revealed in a filing dated September 27 with the U.S. Security and Exchange Commission that an unknown "individual or organization gained unauthorized access to databases within its network on several occasions, and that login information allowing access to or from its Electronic Data Transfer (EDT) environment was compromised for approximately 235 of its customers."

Syniverse repeatedly declined to answer specific questions from Motherboard about the scale of the breach and what specific data was affected, but according to a person who works at a telephone carrier, whoever hacked Syniverse could have had access to metadata such as length and cost, caller and receiver's numbers, the location of the parties in the call, as well as the content of SMS text messages.

Read More on Vice

More #News

- Open source: Google is going to pay developers to make projects more secure
- Google to turn on 2-factor authentication by default for 150 million users
- Poorly Configured Apache Airflow Instances Leak Credentials for Popular Services

- Researchers Discover UEFI Bootkit Targeting Windows Computers Since 2012
- Apple now requires all apps to make it easy for users to delete their accounts
- New U.S. Government Initiative Holds Contractors Accountable for Cybersecurity
- JFrog becomes latest organization authorized as numbering authority for vulnerabilities exposure
- YubiKey Bio builds biometric authentication into a security key
- European Parliament passes non-binding resolution to ban facial recognition
- Amnesty International links cybersecurity firm to spyware operation
- Microsoft is disabling Excel 4.0 macros by default to protect users
- NSA warns of ALPACA TLS attack, use of wildcard TLS certificates
- Botnet abuses TP-Link routers for years in SMS messaging-as-a-service scheme
- Facebook: Outage caused by faulty routing configuration changes
- Ransomware law would require victims to disclose ransom payments within 48 hours

#Breach Log

- Hong Kong firm becomes latest marketing company hit with REvil ransomware
- Twitch source code, business data, gamer payouts leaked in massive hack
- The Telegraph exposes 10 TB database with subscriber info
- Fired IT admin revenge-hacks school by wiping data, changing passwords
- FIN12 hits healthcare with quick and focused ransomware attacks
- Cox Media Group confirms ransomware attack that took down broadcasts
- BrewDog exposed data for over 200,000 shareholders and customers

#Patch Time!

- Code Execution Bug Affects Yamale Python Package — Used by Over 200 Projects
- New Patch Released for Actively Exploited 0-Day Apache Path Traversal to RCE Attacks
- Axis releases updates for three new vulnerabilities found by security company
- Android October patch fixes three critical bugs, 41 flaws in total
- Medtronic urgently recalls insulin pump controllers over hacking concerns
- Unpatched Dahua cams vulnerable to unauthenticated remote access

#Tech and #Tools

- UEFI threats moving to the ESP: Introducing ESPecter bootkit
- Life is Pane: Persistence via Preview Handlers
- Reverse engineering and decrypting CyberArk vault credential files
- Assessing the security and privacy of Vaccine Passports
- kdigger: a Context Discovery Tool for Kubernetes Security Audits
- 23andMe's Yamale Python code injection, and properly sanitizing eval()
- Phrack #70

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