kindred

Security Newsletter

9 March 2020

Subscribe to this newsletter

FCC Proposes to Fine Wireless Carriers $200M for Selling Customer Location Data

The U.S. Federal Communications Commission (FCC) today proposed fines of more than $200 million against the nation's four largest wireless carriers for selling access to their customers' location information without taking adequate precautions to prevent unauthorized access to that data. While the fines would be among the largest the FCC has ever levied, critics say the penalties don't go far enough to deter wireless carriers from continuing to sell customer location data.

The FCC proposed fining T-Mobile $91 million; AT&T faces more than $57 million in fines; Verizon is looking at more than $48 million in penalties; and the FCC said Sprint should pay more than $12 million. An FCC statement (PDF) said "the size of the proposed fines for the four wireless carriers differs based on the length of time each carrier apparently continued to sell access to its customer location information without reasonable safeguards and the number of entities to which each carrier continued to sell such access."

"Time and again, from Facebook to Equifax, massive companies take reckless disregard for Americans' personal information, knowing they can write off comparatively tiny fines as the cost of doing business," Wyden said in a written statement. "The only way to truly protect Americans' personal information is to pass strong privacy legislation like my Mind Your Own Business Act to put teeth into privacy laws and hold CEOs personally responsible for lying about protecting Americans' privacy."

Read More on KrebsOnSecurity

More #News

- Why 'free' Wi-Fi isn't really free
- CrowdStrike's 2020 Threat Report: Spammers fine-tune email thread hijacking

- CrowdStrike's 2020 Threat Report: Spammers fine tune email thread hijacking
- US Drugstore Giant Walgreens Leaked Users' Sensitive Info
- XSS plugin vulnerabilities plague WordPress users
- Digital piggy bank sevice broken into by cybercrooks
- Virgin Media exposes data of 900,000 users via unprotected marketing database
- Microsoft: 99.9% of compromised accounts did not use multi-factor authentication
- Nearly 1 Million Domains Use DMARC, but Only 13% Prevent Email Spoofing
- T-Mobile Data Breach Exposes Customer's Personal, Financial Info
- You Can Now Run Android on an iPhone With 'Project Sandcastle'
- Carnival Cruise Line Operator Discloses Potential Data Breach
- Enhancing Pwned Passwords Privacy with Padding
- J.Crew Disables User Accounts After Credential Stuffing Attack
- Why 3 million Let's Encrypt certificates have been killed off
- Browsers to block access to HTTPS sites using TLS 1.0 and 1.1 starting this month
- Human-operated ransomware attacks: A preventable disaster

#Patch Time!

- Critical PPP Daemon Flaw Opens Most Linux Systems to Remote Hackers
- Hackers Scanning for Apache Tomcat Servers Vulnerable to Ghostcat Attacks
- Nvidia patches severe flaws affecting GeForce, Quadro NVS and Tesla
- Cisco Patches Remote Code Execution Flaws in Webex Player
- Google fixes MediaTek bug in Android March patches

#Tech and #Tools

- Common API security pitfalls
- 31 API security tips - chronological order, raw format
- Best of 2019: Breaking Down the OWASP API Security Top 10, Part 1 | (Part 2)
- Automated IDOR Discovery through Stateful Swagger Fuzzing
- Florentino: Fast Static File Analysis Framework
- dnstwister: Check potential phishing with domain name permutation engine
- Exploiting an SSRF: Trials and Tribulations
- How to scan your WordPress sites for vulnerabilities
- Use Sysmon DNS data for incident response
- CRLite: Finally a fix for broken revocation?
- Addressing the Web's Client-Side Security Challenge
- The threat intelligence handbook
- Malware evasion techniques handbook
- macOS Triage Tool: A DFIR tool to collect artifacts on macOS
- Rita: Real Intelligence Threat Analytics
- MSSQL forensics (1) - MDF fundamentals
- New Attack Vector Targeting Cloud Environment
- ThreatDragon: cross-platform threat modeling application
- ADTimeline: Timeline of Active Directory changes with replication metadata
- CS6038/CS5138 Malware Analysis - free course
- Abusing Slack for Offensive Operations

- Using Splunk as an Offensive Security Tool
- Attacking And Defending The GCPMetadata API
- AWS Automated Remediation - Part 2: S3 Buckets

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

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

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