kindred

Security Newsletter

26 March 2018

Subscribe to this newsletter

Facebook loses control of 50 million users' data, suspends analytics firm

Cambridge Analytica – the data-crunching firm with tools so muscular that founder Christopher Wylie has described it as "Steve Bannon's psychological warfare mindf**k tool" – has been collecting Facebook user data without permission through "a scam and a fraud," Facebook said on Friday.

On Friday, after a week of questions from investigative reporters, Facebook suspended Cambridge Analytica and parent company Strategic Communication Laboratories (SCL) from its platform. The suspensions came late in the game, news outlets are charging, given that Facebook has known about this for three years. Facebook, for its part, claims that the parties involved lied about having deleted harvested data years ago. At least one of the parties involved lied about having deleted harvested data years ago. At least one of the parties involved has shown evidence that points to Facebook having done very little to make sure the data was deleted.

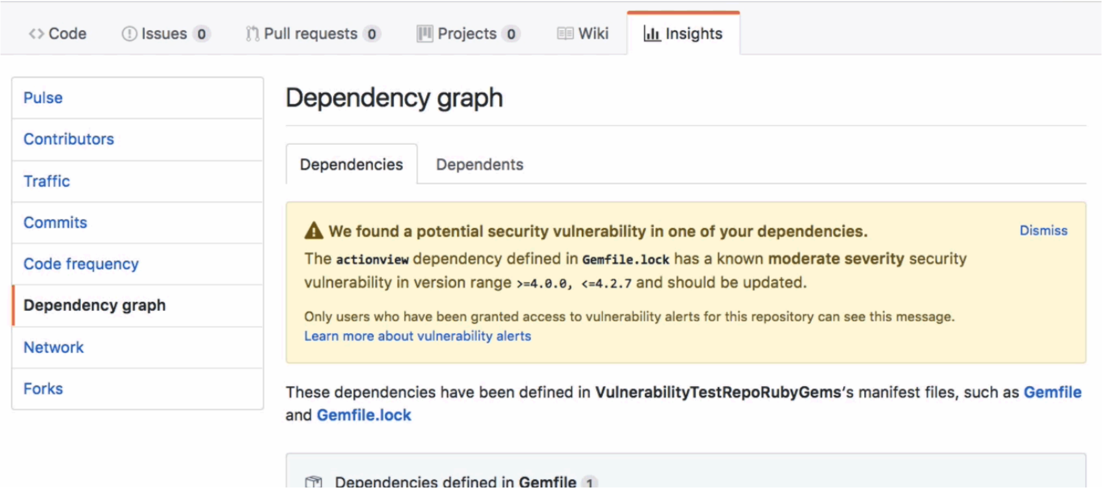
Not surprisingly, Facebook immediately pushed back against the characterization of a massive data leak in an update to its initial announcement of the suspensions. It said that the data got out not through a leak but because some 270,000 Facebook users willingly signed up for a Facebook personality test called thisisyourdigitallife that billed itself as “a research app used by psychologists.” The Observer reports that the dossier includes emails, invoices, contracts and bank transfers that reveal more than 50 million profiles – most of which belong to registered US voters – that were harvested from Facebook. Facebook has suspended Wylie from its platform while it carries out its investigation.

You might well question how 270,000 people signing up for a Facebook personality quiz blossomed into a potential data breach affecting 50 million users – nearly 25% of potential US voters. As The Observer describes it, the app scraped not just test-takers’ private profile data, but also that of their friends. Facebook didn’t disallow such behavior from apps at the time, but such data harvesting was allowed only to improve user experience in the app, not to be sold or used for advertising. Of the 50 million profiles scraped (only 270,000 of which belonged to users who’d granted permission), roughly 30 million contained enough information, including places of residence, that the company could (at least theoretically) match users to other records and build “psychographic” profiles.

Read More

Even More

GitHub dependency security alerts notified developers of 4M code vulnerabilities



Dependency graph

We found a potential security vulnerability in one of your dependencies.

The `actionview` dependency defined in `Gemfile.lock` has a known **moderate severity** security vulnerability in version range `>=4.0.0, <=4.2.7` and should be updated.

Only users who have been granted access to vulnerability alerts for this repository can see this message.
Learn more about vulnerability alerts

These dependencies have been defined in **VulnerabilityTestRepoRubyGems**'s manifest files, such as **Gemfile** and **Gemfile.lock**

Dependencies defined in **Gemfile** 1

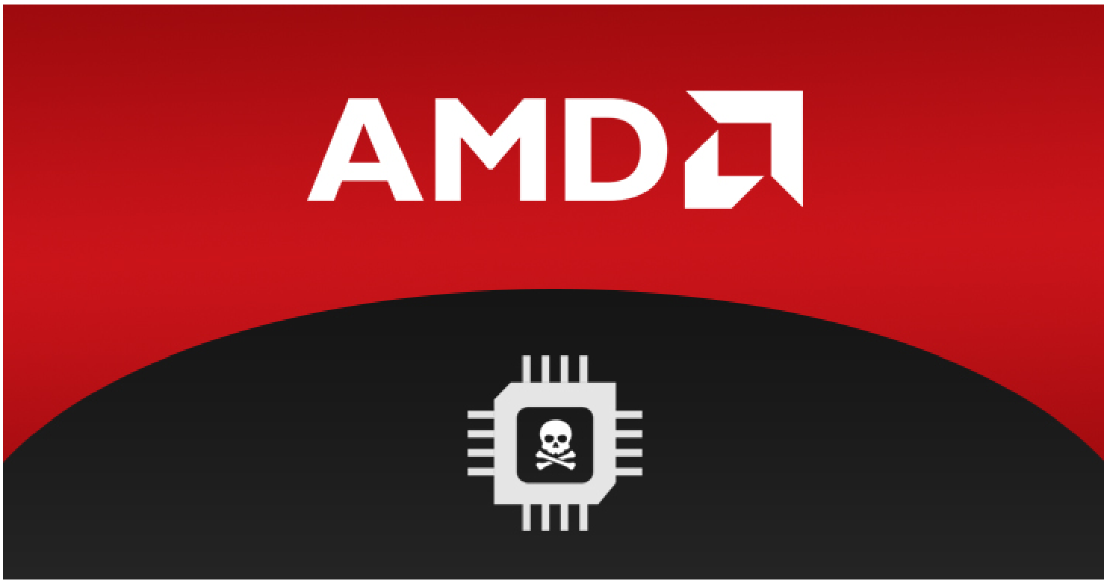
GitHub dependency alerts, which the repository site implemented in November 2017, have notified developers of over four million security vulnerabilities in more than 500,000 Ruby and JavaScript dependencies in the four months since. The alerts, which show up on all RubyGems and JavaScript npm dependencies used by a project, are an essential part of app development security, GitHub said.

Developers who use RubyGems or npm on GitHub should be sure to enable security alerts, and those who use Python should keep an eye out—the alerts will be added to Python dependencies later this year. With over 75% of GitHub projects using shared dependencies, there's a good possibility that at least one of the projects you're involved in could benefit from security alerts. They aren't enabled by default, however, so you'll need to toggle a few settings to turn them on. With more than 500,000 libraries being vulnerable to upwards of four million issues there's a good chance code you're involved with is affected, and GitHub is making it easy to fix the problem.

Read More

Even More

AMD Acknowledges Newly Disclosed Flaws In Its Processors — Patches Coming Soon



AMD has finally acknowledged 13 critical vulnerabilities, and exploitable backdoors in its Ryzen and EPYC processors disclosed earlier this month by Israel-based CTS Labs and promised to roll out firmware patches for millions of affected devices ‘in the coming weeks.’

According to CTS-Labs researchers, critical vulnerabilities (RyzenFall, MasterKey, Fallout, and Chimera) that affect AMD's Platform Security Processor (PSP) could allow attackers to access sensitive data, install persistent malware inside the chip, and gain full access to the compromised systems. In a press release published by AMD on Tuesday, the company downplays the threat by saying that, "any attacker gaining unauthorised administrative access would have a wide range of attacks at their disposal well beyond the exploits identified in this research."

Infosec experts and journalists embroiled CTS Labs into controversies by raising questions over the way it disclosed vulnerabilities details to the public in less than 24 hours after notifying AMD. According to Ilia Luk-Zilberman, CTO of CTS-Labs, the current process of 'Responsible Disclosure' has two significant problems: 1) If researcher gives a 30/45/90 days limit to the affected vendor, it's extremely rare that the vendor would notify its customers about the unpatched security vulnerabilities during this period, leaving them unaware of potential risks. 2)If vendors do not respond or patch the vulnerability during this 90-day disclosure period, researchers can proudly prefer to go public with full technical details of the flaws, ultimately putting their customers at risk.

Read More

Press release

Cutting room floor

- Hackers leave ransom note after wiping out MongoDB in 13 seconds
- Unified Logs in High Sierra (10.13) Show Plaintext Password for APFS Encrypted External Volumes via Disk Utility.app
- Online Sandboxing: A Stash for Exfiltrated Data?
- How Serverless Computing Reshapes Security
- Google bolsters security tools on Google Cloud, G Suite
- New R2D2 Technique Protects Files Against Wiper Malware
- Hackers pwn Edge, Firefox, Safari, macOS, VirtualBox at Pwn2Own 2018
- 15-Year-old Finds Flaw in Ledger Crypto Wallet
- Apple Blocks Sites From Abusing HSTS Security Standard to Track Users
- Windows Remote Assistance Exploit Lets Hackers Steal Sensitive Files
- Thousands of servers found leaking 750MB worth of passwords and keys
- Mozilla Is Testing "DNS over HTTPS" Support in Firefox
- 880,000 payment cards affected in travel company data breach

#Tech and #Tools

- Hardentools: disables a number of risky Windows features
- APT2: Automated penetration toolkit
- Introducing Endgame Red Team Automation
- Real-time certificate transparency log update stream.
- We need to talk about IDS signatures
- Sandbox awareness via user behaviour
- Vshadow: Abusing the Volume Shadow Service for Evasion, Persistence, and Active Directory Database Extraction
- Deep dive on the most severe Kubernetes vulnerabilities to date
- Ending DNS Hijacking with DNSCrypt

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 over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and 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 as an innovation driven company that builds on trust.

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