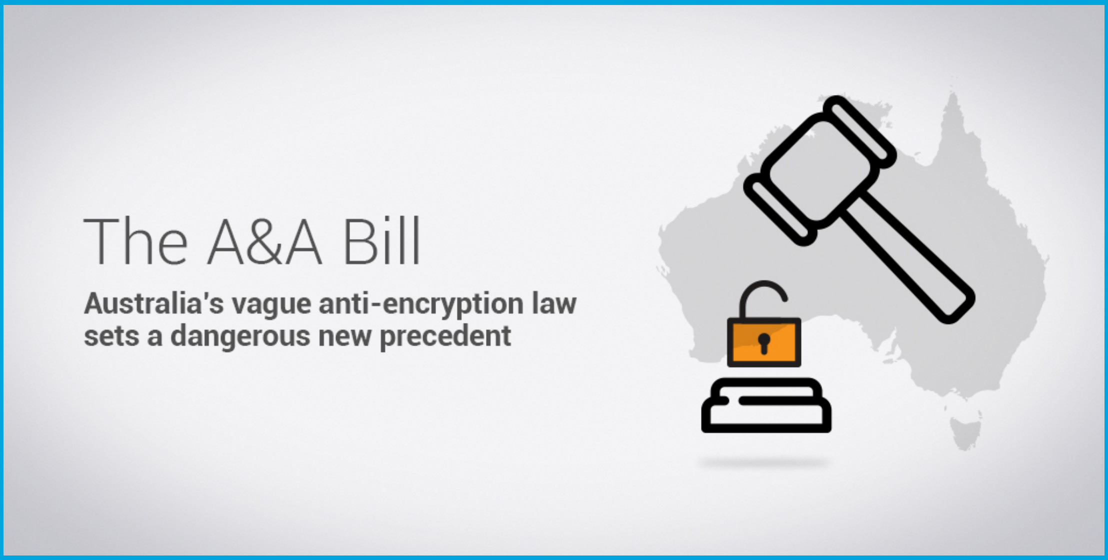
kindred

Security Newsletter

17 December 2018

Subscribe to this newsletter

What's actually in Australia's encryption laws?


The A&A Bill
Australia's vague anti-encryption law sets a dangerous new precedent

Labor caved in last Thursday. Despite spending hours telling Parliament why the Assistance and Access Bill was dangerous garbage, and complaining about the rushed process, they dropped all of their proposed amendments and voted in the sitting government's version anyway. The most controversial part is the "frameworks for voluntary and mandatory industry assistance to law enforcement and intelligence agencies" to help government access the content of encrypted communications.

Under the new laws, Australian government agencies can issue three kinds of notices: Technical Assistance Notices (TAN), which are compulsory notices for a "designated communication provider" to use an interception capability they already have; Technical Capability Notices (TCN), which are compulsory notices for a designated communication provider to build a new interception capability, so that it can meet subsequent Technical Assistance Notices; and Technical Assistance Requests (TAR), which are "voluntary" requests, but which have been described by experts as the most dangerous of the three because there was less oversight, at least in the original version of the law.

Is this about fighting terrorism and child abuse? Kinda. It includes any crime "punishable by a maximum term of imprisonment of 3 years or more or for life". ASIS can also ask for assistance in relation to "the interests of Australia's foreign relations or the interests of Australia's national economic well-being".

Who's impacted? Pretty much anyone and everyone who provides any kind of online service or communications equipment to anyone in Australia, and anyone who even installs or maintains the kit. Yes, that includes anyone who has a website.

Read More on ZDNet

Even More on ProtonMail Blog

Google+ to Shut Down Early After New API Flaw potentially impacts 52.5 Million Users

Google said it discovered another critical security vulnerability in one of Google+'s People APIs that could have allowed developers to steal private information on 52.5 million users, including their name, email address, occupation, and age.

The vulnerable API in question is called "People: get" that has been designed to let developers request basic information associated with a user profile .However, software update in November introduced the bug in the Google+ People API that allowed apps to view users' information even if a user profile was set to not-public. Google engineers discovered the security issue during standard testing procedures and addressed it within a week of the issue being introduced.

The company said it found no evidence that the vulnerability was exploited or its users' data was misused by any third-party app developers. Google also assured its users that no passwords, financial data, national identification numbers or any other sensitive data were left exposed by this API bug. Google said the company is going to shut down its social media network in April 2019 instead of August.

Read More on TheHackerNews

Even More on ArsTechnica

More #News

- Text CAPTCHAs easily beaten by neural networks
- New LamePyre macOS Malware Sends Screenshots to Attacker
- Spammed Bomb Threat Hoax Demands Bitcoin
- Logitech app security flaw allowed keystroke injection attacks
- Apps on smartphones are selling and sharing our location data 24/7
- Ships infected with ransomware, USB malware, worms
- Scanning for Flaws, Scoring for Security
- Researchers Find a Dozen Undocumented OpenSSH Backdoors
- Cryptography failure leads to easy hacking for PlayStation Classic
- Hackers Using Formjacking Technique to Steal Credit Card Details from Payment Forms
- Mac Malware Cracks WatchGuard's Top 10 List
- Ticketmaster tells customer it's not at fault for site's Magecart malware pwnage

#Patch Time!

- Patch Tuesday, December 2018 Edition
- Adobe's Year-End Update Patches 87 Flaws in Acrobat Software
- WordPress plugs bug that led to Google indexing some user passwords
- phpMyAdmin Releases Critical Software Update — Patch Your Sites Now!

#Tech and #Tools

- Protecting Your Site With Feature Policy
- 50 CVEs in 50 Days: Fuzzing Adobe Reader
- CVE-2018-8626 | Windows DNS Server Heap Overflow Vulnerability
- change-password-url Specifications
- From blind XXE to root-level file read access
- Your Culture is in Your Password: An Analysis of a Demographically-diverse Password Dataset
- How Equifax breach happened
- Step Certificates: An open source solution for secure automated certificate management
- Persistent XSRF on Kubernetes Dashboard using Redhat Keycloak Gatekeeper on Microsof Azure
- Implementation of the OWASP Mobile TOP 10 methodology for testing Android applications
- Uberducky - a wireless USB Rubber Ducky triggered via BLE

This is the last Kindred Security Newsletter for 2018

It's time for the Kindred Group Security team to take some holiday. The newsletter will be off for a few weeks during Christmas and New Year's Eve. But don't worry, we'll be back. See you soon for some awesome infosec news!

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 24 million customers across 100 markets. 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 as an innovation driven company that builds on trust.

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