kindred

Security Newsletter

6 November 2017

Subscribe to this newsletter

iPhones get a KRACK patch and a critical Wi-Fi 0-day on the same day

Yesterday, Apple treated its customers to a number of security updates across several products. This included a fix for the Wi-Fi-related vulnerability known as KRACK, which is available for some – but not all – iOS devices. The CVE that Apple addresses with its fix for KRACK is CVE-2017-13080, one of the several KRACK-related CVEs.

The even bigger news is what Apple didn't address: an iOS Wi-Fi 0-day (yes, another one) that emerged yesterday from the annual Mobile Pwn2Own hacking competition.

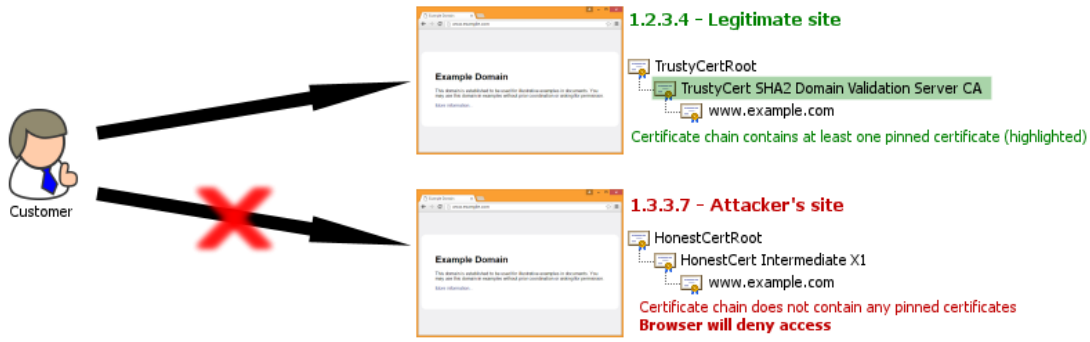
Zero Day Initiative reports that Tencent Keen Security Lab gets code execution through a Wi-Fi bug and escalates privileges to persist through a reboot. Tencent Keen Security Lab earned a cool $110,000 for their trouble while Apple now has just 90 days to fix the problem festering on our iPhones before details are made public.

Users of El Capitan (macOS 10.11.6) and Sierra (10.12.6) should install the latest operating system security updates – 2017-004 for El Capitan, 2017-001 for Sierra. High Sierra (10.13) users should update to version 10.13.1 to receive these fixes.

Read More

Krack Wi-fi Vulnerability Explained

RIP HPKP: Google abandons public key pinning



Google has announced plans to deprecate Chrome support for HTTP public key pinning (HPKP), an IETF standard that Google engineers wrote to improve web security but now consider harmful.

HTTP Public Key Pinning (HPKP) is a standard that allows a host to instruct browsers to only accept certain public keys when communicating with it for a given period of time. WSecurity researchers have highlighted a number of problems with HPKP, including the possibility for an attacker to install malicious pins or for a site operator to accidentally block visitors.

Currently Chrome, Firefox, and Opera are the only browsers that support HPKP, but Google's Chrome security team have announced plans to remove support for HPKP in Chrome 67, which is due for stable release around May 29, 2018.

Instead of pinning, the Chrome team are now encouraging developers to use Certificate Transparency and the relatively new Expect-CT header.

Read More

The death knell for HPKP?

Highly Critical Flaw (CVSS Score 10) Lets Hackers Hijack Oracle Identity Manager

A highly critical vulnerability has been discovered in Oracle's enterprise identity management system that can be easily exploited by remote, unauthenticated attackers to take full control over the affected systems. The critical vulnerability tracked as CVE-2017-10151, has been assigned the highest CVSS score of 10 and is easy to exploit without any user interaction.

The security loophole is due to a "default account" that an unauthenticated attacker over the same network can access via HTTP to compromise Oracle Identity Manager. Oracle has not released complete details of the vulnerability in an effort to prevent exploitation in the wild, but here the "default account" could be a secret account with hard-coded or no password.

The easily exploitable vulnerability affects Oracle Identity Manager versions 11.1.1.7, 11.1.1.9, 11.1.2.1.0, 11.1.2.2.0, 11.1.2.3.0 and 12.2.1.3.0. Oracle has released patches for all versions of its affected products, so you are advised to install the patches before hackers get a chance to exploit the vulnerability to target your enterprise.

Read More

Heathrow probe after 'security files found on USB stick

Heathrow Airport says it has launched an internal investigation after a USB stick containing security information was reportedly found on the street. The USB stick had 76 folders with maps, videos and documents, including details of measures used to protect the Queen.

Some files disclosed the types of ID needed to access restricted areas, a timetable of security patrols and maps pinpointing CCTV cameras. One document highlighted recent terror attacks and talked about the type of threat the airport could face.

Statement from the airport: "The UK and Heathrow have some of the most robust aviation security measures in the world, and we remain vigilant to evolving threats by updating our procedures on a daily basis."

Read More

Report: Average business user must keep track of 191 passwords

The average business employee must keep track of 191 passwords, according to a report from password management firm LastPass, released Wednesday. That's seven times higher than standard industry reports, which report the average is 27 passwords.

People often underestimate the number of accounts they actually have, according to the report. For example, marketing professionals use several advertising and analytics platforms, while systems administrators manage different services, and sales representatives set up demo accounts on a regular basis.

Only 27% of businesses have enabled multi-factor authentication to protect their password vaults, LastPass found. "While we're seeing that a significant portion of businesses are investing in multi-factor authentication, it is not yet adopted widely enough to compensate for the shortcomings of passwords," the report stated.

Read More

Virtually everyone in Malaysia pwned in telco, govt data hack spree

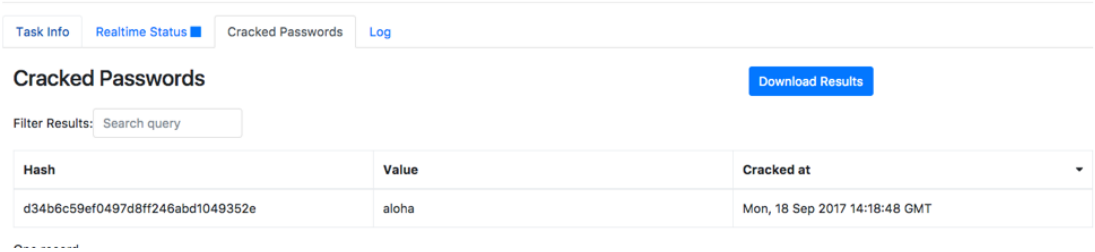
Information on 46.2 million cellphone accounts was slurped from Malaysians telecoms providers. To put that in context, the population of Malaysia is 31.2 million; obviously, some people have more than one number.

The stolen telco records include people's mobile phone numbers, SIM card details, device serial numbers, and home addresses, all of which are useful to identity thieves and scammers. Some 80,000 medical records were also accessed during the hacking spree, and government websites as well as Jobstreet.com were attacked and infiltrated too.

Incredible as it may seem there's at least a couple of precedents for a huge chunk of the population of an entire country getting caught up in a database security breach. The personal records of millions of folks in South Africa spilled online only last month. Almost everyone who had a credit card in South Korea was pwned back in 2014 in another unedifying security cockup.

Read More

Introducing GoCrack: A Managed Password Cracking Tool



FireEye's Innovation and Custom Engineering (ICE) team released a tool today called GoCrack that allows red teams to efficiently manage password cracking tasks across multiple GPU servers by providing an easy-to-use, web-based real-time UI (Figure 1 shows the dashboard) to create, view, and manage tasks. Simply deploy a GoCrack server along with a worker on every GPU/CPU capable machine and the system will automatically distribute tasks across those GPU/CPU machines.

Password cracking tools are an effective way for security professionals to test password effectiveness, develop improved methods to securely store passwords, and audit current password requirements. Some use cases for a password cracking tool can include cracking passwords on exfil archives, auditing password requirements in internal tools, and offensive/defensive operations.

GoCrack is shipping with support for hashcat v3.6+, requires no external database server (via a flat file), and includes support for both LDAP and database backed authentication. The server component can run on any Linux server with Docker installed. Users with NVIDIA GPUs can use NVIDIA Docker to run the worker in a container with full access to the GPUs. GoCrack is available immediately for download along with its source code on the project's GitHub page.

Read More

Cutting room floor

- Disclosure: WordPress WPDB SQL Injection - Technical
- Slack SAML authentication bypass
- Yubico launches YubiHSM 2: The smallest, cheapest Hardware Security Module (HSM)
- A flaw in Google's bug database exposed private security vulnerability reports
- Researchers Devise 2FA System That Relies on Taking Photos of Ordinary Objects
- "Silence" Trojan Records Pseudo-Videos of Bank PCs to Aid Bank Cyber-Heists
- Just one day after its release, iOS 11.1 hacked by security researchers
- Bypassing Browser Security Warnings with Pseudo Password Fields
- Now anyone can fool reCAPTCHA

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