kindred

Security Newsletter

15 January 2018

Subscribe to this newsletter

Meltdown / Spectre: Almost all CPUs since 1995 vulnerable to these attacks

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents. Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers.

The bugs were discovered by Jann Horn, a security researcher with Google Project Zero. Horn describes these issues as hardware bugs that will need both firmware patches from CPU vendors and software fixes from both OS and application vendors. According to Google, everything and everyone is affected. This includes all major chipset vendors (Intel, AMD, ARM), all major operating systems (Windows, Linux, macOS, Android, ChromeOS), cloud providers (Amazon, Google, Microsoft), and application makers.

The actual flaws reside in a technique called "speculative execution" that is employed by all modern CPUs. This is a basic optimization technique that processors employ to carry out computations for data they "speculate" may be useful in the future. Google says that Horn discovered a way to use speculative execution to read data from the CPU's memory that should have not been available for user-level apps.

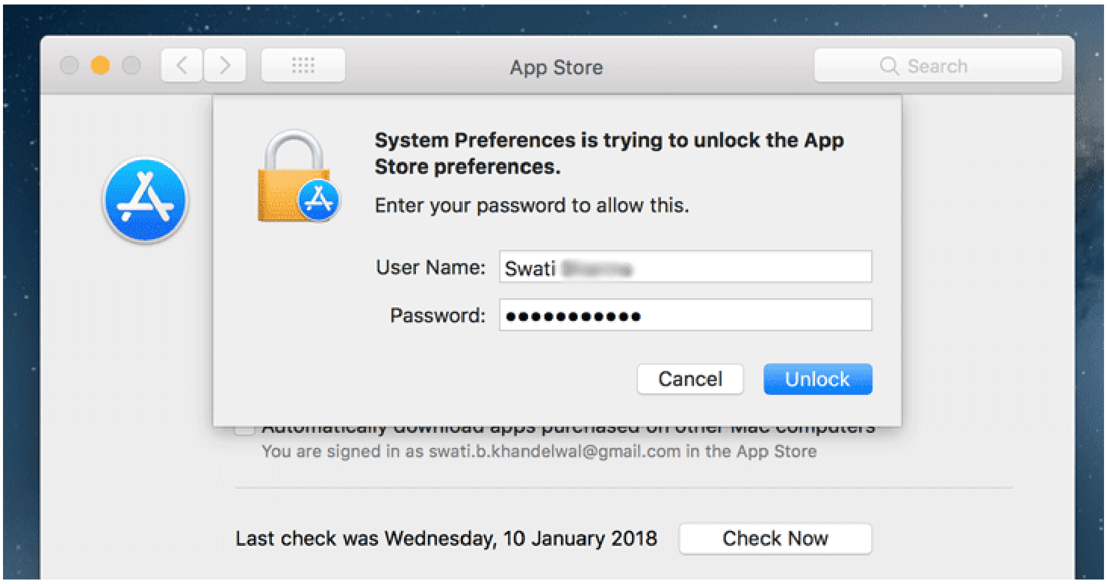
Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.**Spectre** breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre.

Read More

"Official" page

Meltdown / Spectre explanation for non-technical audience

2018 - Bad start for MacOS as well



System Preferences is trying to unlock the App Store preferences.

Enter your password to allow this.

User Name: Swati [redacted]

Password: ●●●●●●●●●●●●

□ Automatically download apps purchased on other Mac computers

You are signed in as swati.b.khandelwal@gmail.com in the App Store

Last check was Wednesday, 10 January 2018

Yet another password vulnerability has been uncovered in macOS High Sierra, which unlocks App Store System Preferences with any password (or no password at all). The vulnerability impacts macOS version 10.13.2 and requires the attacker to be logged in with an administrator-level account for this vulnerability to work.

Apple also patched a similar vulnerability in October in macOS, which affected encrypted volumes using APFS wherein the password hint section was showing the actual password of the user in the plain text. There was also the root login bug in Apple's desktop OS that enabled access to the root superuser account simply by entering a blank password on macOS High Sierra 10.13.1. What's wrong with password prompts in macOS? It's high time Apple should stop shipping updates with such an embarrassing bug.

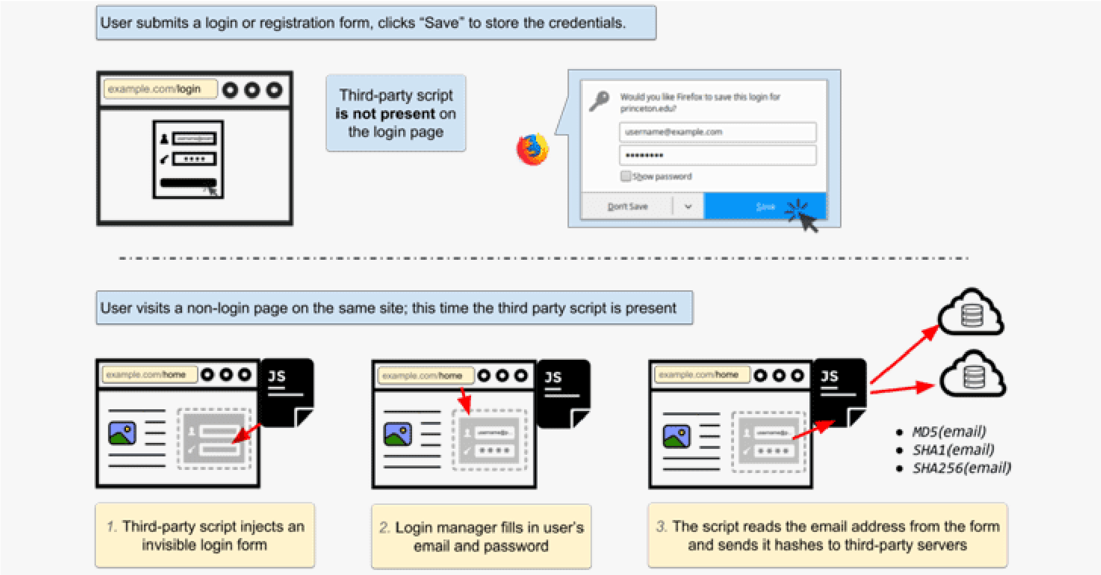
A few days ago, a researcher ended 2017 with a bang by releasing details of a macOS kernel exploit, based on an IOHIDFamily zero-day, that affects all Mac operating systems. The bug is a local privilege escalation (LPE) flaw that can be exploited only if an attacker has local access to the Mac — or previously pwned the computer. However, exploiting it would give an attacker root access.

The researcher said "I would've submitted to Apple if their bug bounty included macOS."

App Store preferences can be unlocked without a password

15-years old MacOS 0-day leads to full system compromise

Flaw In Major Browsers Allows 3rd-Party Scripts to Steal Your Saved Passwords



User submits a login or registration form, clicks "Save" to store the credentials.

Third-party script **is not present** on the login page

User visits a non-login page on the same site; this time the third party script is present

1. Third-party script injects an invisible login form

2. Login manager fills in user's email and password

3. The script reads the email address from the form and sends it hashes to third-party servers

Security researchers have uncovered how marketing companies have started exploiting an 11-year-old bug in browsers' built-in password managers, which allow them to secretly steal your email address for targeted advertising across different browsers and devices.

Every modern browser—Google Chrome, Mozilla Firefox, Opera or Microsoft Edge—today comes with a built-in easy-to-use password manager tool that allows you to save your login information for automatic form-filling. Third-party tracking scripts found by researchers inject invisible login forms in the background of the webpage, tricking browser-based password managers into auto-filling the form using the saved user's information. Since these scripts are primarily designed for user-tracking, they detect the username and send it to third-party servers after hashing with MD5, SHA1 and SHA256 algorithms, which could then be used as a persistent ID for a specific user to track him/her from page to page.

Although the researchers have spotted marketing firms scooping up your usernames using such tracking scripts, there is no technical measure to prevent these scripts from collecting your passwords the same way. The simplest way to prevent such attacks is to disable the autofill function on your browser.

Read More

Login Manager autofill abuse demo page

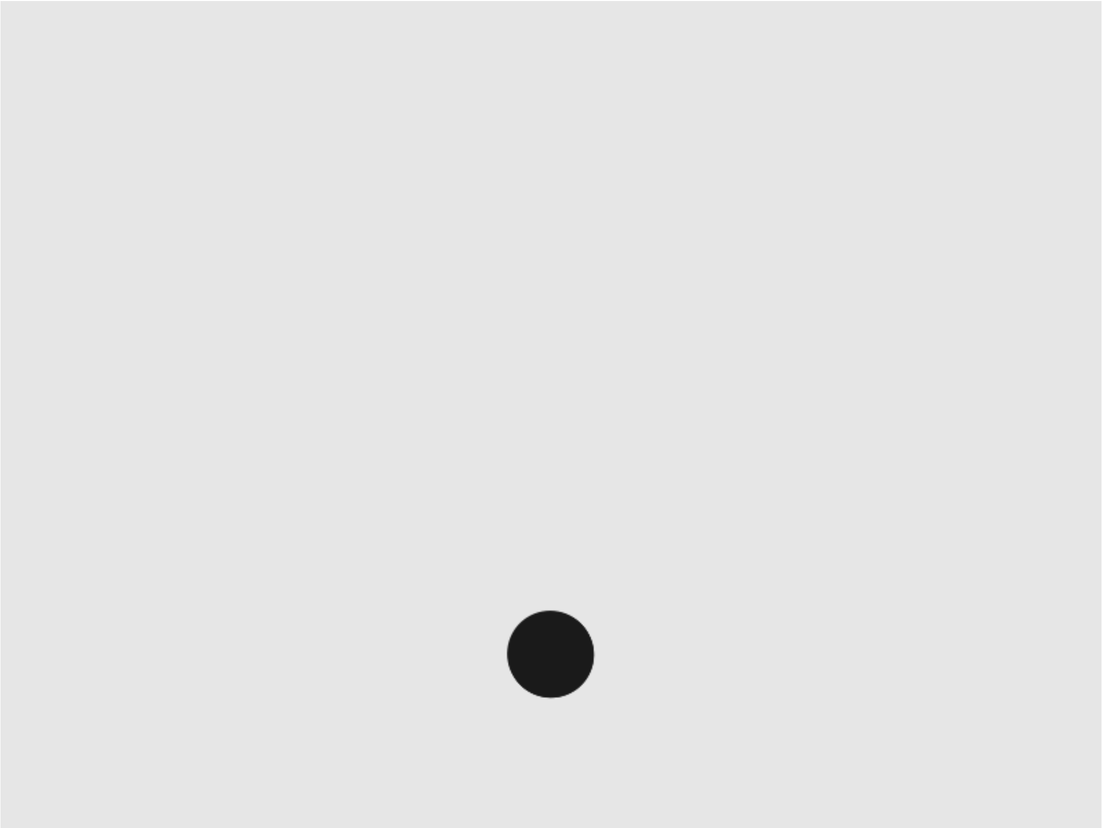
VTech hack fallout: What is a kid's privacy worth? About 22 cents – FTC

The US Federal Trade Commission (FTC) today agreed to a settlement deal with a children's electronic toymaker it had accused of collecting kids' personal information and then failing to properly secure that data. The government watchdog said VTech will pay $650,000 and agree to a set of privacy and security requirements in order to settle charges it violated both the Children's Online Privacy Protection Act (COPPA) and the FTC Act. VTech will also agree to a stricter set of compliance requirements, including regular third-party security audits to check whether it is properly storing and encrypting its collected information, and to make sure it is getting express consent from parents before it collects and personal information.

The breached Learning Lodge and Kid Connect services were said to have hosted around 2.25 million accounts that contained information on roughly three million kids. The accounts had things like the child's name, date of birth, and gender as well as the parent's name, physical address, email address, and security question answers. VTech was accused of failing to properly encrypt that information (a violation of COPPA) and lying to parents about the extent of data collection and level of security it used (a violation of the FTC Act).

Read More

With WPA3, Wi-Fi security is about to get a lot tougher



The Wi-Fi Alliance, an industry body made up of device makers, announced monday its next-generation wireless network security standard, WPA3. The standard will replace WPA2, a near-two decades-old security protocol that's built in to protect almost every wireless device today -- including phones, laptops, and the Internet of Things.

One of the key improvements in WPA3 will aim to solve a common security problem: open Wi-Fi networks. Seen in coffee shops and airports, open Wi-Fi networks are convenient but unencrypted, allowing anyone on the same network to intercept data sent from other devices. WPA3 employs individualized data encryption, which scramble the connection between each device on the network and the router, ensuring secrets are kept safe and sites that you visit haven't been manipulated.

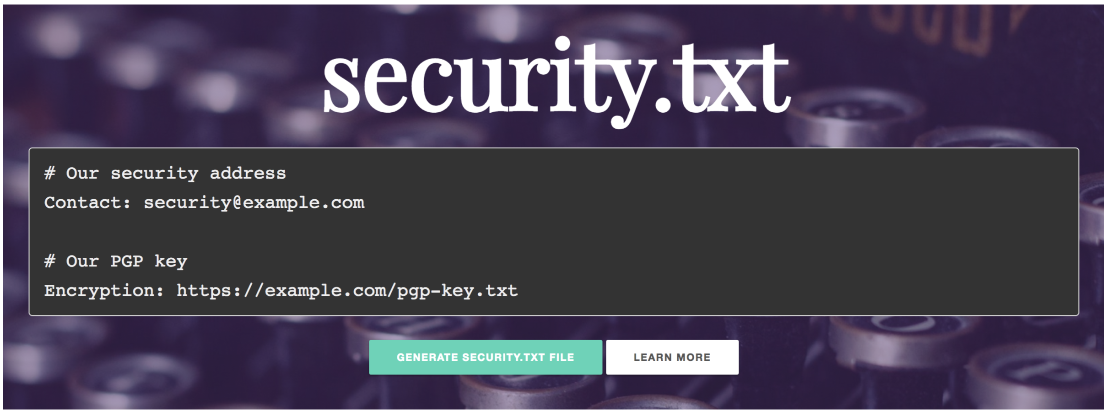
Another key improvement in WPA3 will protect against offline brute-force dictionary attacks, making it tougher for attackers near your Wi-Fi network to guess a list of possible passwords. The new wireless security protocol will also block an attacker after too many failed password guesses.

The new WPA3 security standard is expected to land in devices later this year.

Read More

Even More

Say hello to security.txt



```
# Our security address
Contact: security@example.com

# Our PGP key
Encryption: https://example.com/pgp-key.txt
```

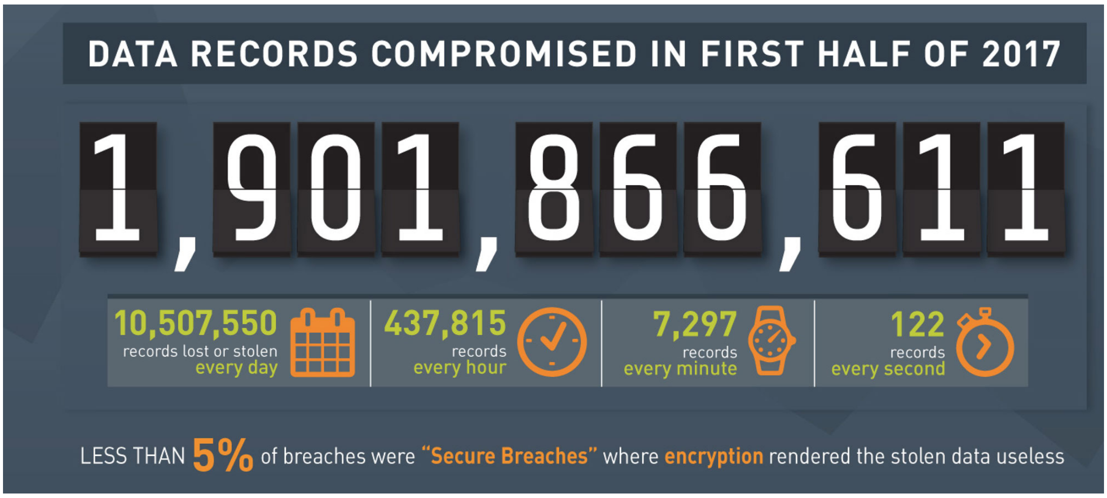
“When security risks in web services are discovered by independent security researchers who understand the severity of the risk, they often lack the channels to disclose them properly. As a result, security issues may be left unreported. Security.txt defines a standard to help organizations define the process for security researchers to disclose security vulnerabilities securely.”

The security.txt file is a simple text file, much like robots.txt, that contains crucial information on who to contact or where to look for security related information about a website. You can read the RFC and check out the securitytxt.org website for more details. That simple little piece of information gives a researcher exactly the information they need should they ever want to contact you.

Read More

Project page

Fixing Data Breaches



We have a data breach problem. They're constant news headlines, they're impacting all of us and frankly, things aren't getting any better. Quite the opposite, in fact - things are going downhill in a hurry. In this 5-parts blog series, you'll find recommendations on how we can address the root causes of data breaches

- Fixing Data Breaches Part 1: Education
- Fixing Data Breaches Part 2: Data Ownership & Minimisation
- Fixing Data Breaches Part 3: The Ease of Disclosure
- Fixing Data Breaches Part 4: Bug Bounties
- Fixing Data Breaches Part 5: Penalties

Cutting room floor

- List of websites and whether or not they support 2FA.
- WhatsApp Flaw Could Allow 'Potential Attackers' to Spy On Encrypted Group Chats
- Cierge: "passwordless" open source authentication server (OIDC)
- Microsoft Releases Patches for 16 Critical Flaws, Including a Zero-Day
- "Trackmageddon" Vulnerabilities Discovered in (GPS) Location Tracking Services
- Demystifying Two Factor Auth
- Setting up a DNS Firewall on steroids
- Ropchain - How to bypass ASLR+DEP+stack canaries

More Spectre / Meltdown stuff

- Windows' antivirus security update compatibility matrix
- Meltdown and Spectre: Here's what Intel, Apple, Microsoft, others are doing about it
- How to Check and Update Windows Systems for the Meltdown and Spectre CPU Flaws
- Meltdown and Spectre – enterprise action plan
- Detecting Spectre And Meltdown Using Hardware Performance Counters
- Meltdown, Spectre and your browser: Edge/Firefox/Chrome/Safari
- What Spectre and Meltdown Mean For WebKit
- CPU security bugs caused by speculative execution
- Spectre - Meltdown Checker Shell script
- Spectre - Meltdown checker - Splunk UF script
- Platform-Agnostic Security Tokens

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