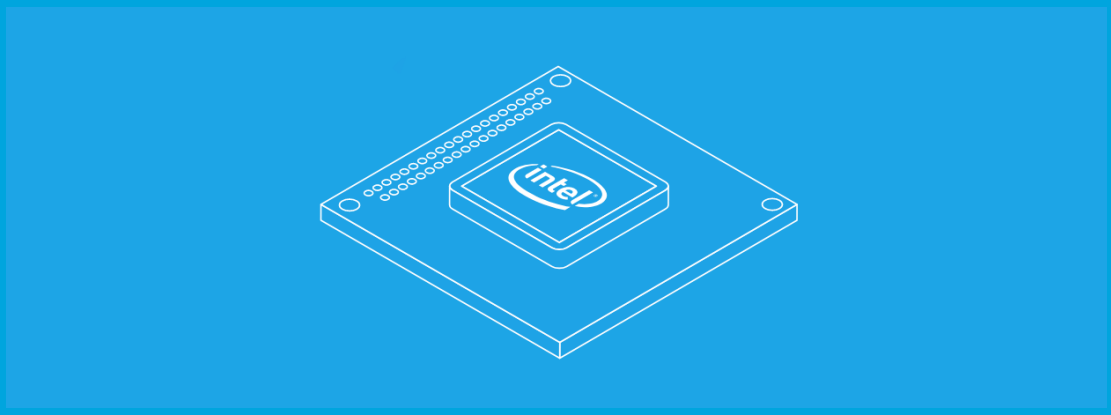
Security Newsletter

18 June 2018

Subscribe to this newsletter

New 'Lazy FP State Restore' Vulnerability Found in All Modern Intel CPUs



Another security vulnerability has been discovered in Intel chips that affects the processor's speculative execution technology—like Specter and Meltdown—and could potentially be exploited to access sensitive information, including encryption related data. Dubbed Lazy FP State Restore, the vulnerability (CVE-2018-3665) within Intel Core and Xeon processors has just been confirmed by Intel, and vendors are now rushing to roll out security updates in order to fix the flaw and keep their customers protected.

As the name suggests, the flaw leverages a system performance optimization feature, called Lazy FP state restore, embedded in modern processors, which is responsible for saving or restoring the FPU state of each running application 'lazily' when switching from one application to another, instead of doing it 'eagerly.'

However, it should be noted that, unlike Spectre and Meltdown, the latest vulnerability does not reside in the hardware. So, the flaw can be fixed by pushing patches for various operating systems without requiring new CPU microcodes from Intel. According to Intel, since the flaw is similar to Spectre Variant 3A (Rogue System Register Read), many operating systems and hypervisor software have already addressed it. AMD processors are not affected by this issue.

Read More

Microsoft Security Advisory

Football app tracks illegal broadcasts using your microphone and GPS

The organization behind Spain's top-flight soccer league known as La Liga has added a functionality to its official Android app that enables it to identify bars, restaurants and other public venues that broadcast soccer games illegally. It has turned out that, after being downloaded or updated, the app asks the user for permission to access their smartphone's microphone and geolocation service (GPS).

If the user grants their permission, La Liga receives the ability to activate the phone's microphone remotely in order to record audio clips of the handset's surroundings. In doing so, the app seeks to ascertain if the captured sound corresponds to that of the broadcast of a soccer game. At the same time, by turning on the phone's geolocation service it can pinpoint the location of the place where the recording was made and, thus, identify the establishment that may be showing the game without a license.

La Liga's governing body, LFP, said in its statement on Monday that the functionality was added to its Android app only in the June 8 update with the sole aim of cracking down on unauthorized broadcasts of soccer games within Spain. La Liga says that unlicensed broadcasts of soccer games in bars and restaurants cost Spanish soccer €150 million (US$176 million) in lost revenues each year.

In an effort to further ease privacy concerns, La Liga said that it doesn't access the captured audio snippet, as the snippet is instead automatically converted into a binary code on the device itself. The code is then compared to a reference database and, if there's no match between the two, the former code is discarded. The organization stressed that there is no way to turn the code back into the actual content of the recording.

Read More

Even More

Cutting room floor

- Kaspersky Halts Europol and NoMoreRansom Project Coop After EU Parliament Vote
- Microsoft Patch Tuesday, June 2018 Edition
- Microsoft Explains Whether a Vulnerability Turns Into a Windows Security Update
- 6 million cards compromised in Dixons Carphone breach
- 17 Backdoored Docker Images Removed From Docker Hub
- The Google Pixelbook power button is now a 2FA token
- Europol Dismantles One of the Internet's Oldest Hacker Groups
- Clipboard Hijacker Targeting Bitcoin & Ethereum Users
- Cortana Hack Lets You Change Passwords on Locked PCs
- The Best English Security Podcasts in 2018
- Android App Devs Find Clever Trick for Fooling Users Into Installing Their Crapware
- Containerized Apps: An 8-Point Security Checklist
- Chinese hackers attack National Data Center using watering hole attack
- GnuPG patched to thwart 'fake filename'

#Tech and #Tools

- BlackHat Europe 2018
- SafeSpec: Banishing the Spectre of a Meltdown with Leakage-Free Speculation
- Kubernetes RBAC plugin
- Server-Side Spreadsheet Injection – Formula Injection to RCE
- Pentester's Windows NTFS tricks collection
- SigSpoof: Spoofing signatures in GnuPG, Enigmail, GPGTools and python-gnupg (CVE-2018-12020)
- Cookies for dummies Part 3: Understanding security flags

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our SOC analyst position
- You're into identity and access management? We are looking for an IAM Specialist
- Interested in Governance, Risk and Compliance? Apply for our InfoSec team

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. You can find all our open vacancies on our career page.

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