Researchers Disclose New 'Inverse Spectre Attack' (digitaljournal.com)

Posted by EditorDavid on Saturday August 11, 2018 @06:34PM from the return-addresses dept.

A new Intel security flaw has been discovered that potentially allows passwords to be stolen. An anonymous reader quotes *Digital Journal: As EE News reports, researchers said the new flaw enables an "inverse spectre attack". According to Giorgi Maisuradze and Professor Dr. Christian Rossow a* `ret2spec` *(return-to-speculation) vulnerability with the chips allows for would-be attackers to read data without authorization. According to Professor Rossow: "The security gap is caused by CPUs predicting a so-called return address for runtime optimization."*

The implications of this are: "If an attacker can manipulate this prediction, he gains control over speculatively executed program code. It can read out data via side channels that should actually be protected from access." This means, in essence, that malicious web pages could intergret the memory of the web browser in order to access and copy critical data. Such data would include stored passwords.

"At least all Intel processors of the past ten years are affected by the vulnerabilities," reports EE News, adding "Similar attack mechanisms could probably also be derived for ARM and AMD processors...."

"Manufacturers were notified of the weaknesses in May 2018 and were granted 90 days to remedy them before the results were published. That deadline has now expired."

bug intel security

→

Cryptocurrency Markets Lost $18 Billion Overnight

Many Enterprise Mobile Devices Will Never Be Patched Against Meltdown, Spectre

Changes in WebAssembly Could Render Meltdown and Spectre Browser Patches Useless

New Spectre 1.1 and Spectre 1.2 CPU Flaws Disclosed

Chrome is Using 10-13% More RAM to Fight Spectre

Theme Park Deploys Trained Crows To Collect Litter

Researchers Disclose New 'Inverse Spectre Attack' More | Reply Login

Researchers Disclose New 'Inverse Spectre Attack'

Post Load All Comments

3 of 88 Comments Hidden Create an Account

Comments Filter:
Score:
5 insightful
4 informative
3 interesting
2 funny

The Fine Print: The following comments are owned by whoever posted them. We are not responsible for them in any way.

- **Re: (Score:2)**
  by AHuxley (892839)
  Back to the mainframe next to the computer with everything written out. Type in everyday as needed due to that CPU.
  - **Re: (Score:2)**
    by Anonymous Coward
    Any clout the brand had has been destroyed in the past year. What shoddy system design.
    1 hidden comment
- **Could probably... (Score:1)**
  by Anonymous Coward
  How much is intel paying for the AMD FUD this time?
- **Realistic solution if you have no money? (Score:1)**
  by Anonymous Coward
  I can barely afford an old Core2Duo for 50 bucks (case and all). And I have actually for real been a target of my own country. How the hell am I supposed to mitigate all this? I run a well-"secured" Linux with at least daily updates of everything, but what's the point? Sure, a few of those bugs can be worked-around in software. But what does it matter? It takes a single proper one, and I'm done.
  I can only console myself with the fact, that if nothing happened until now, then nothing may happen. But I just c
  7 hidden comments
  - **Re: Realistic solution if you have no money? (Score:2)**
    by Gappy (12314)
    Use an old processor without speculative execution features? Some lower end ARMs and Atoms also are immune, I think.
    3 hidden comments
  - **Re: (Score:1)**
    by drinkypoo (153816)
    I can barely afford an old Core2Duo for 50 bucks (case and all).
    Should have bought an old Athlon for fifty bucks instead. Lots of us tried to tell you that Intel was unscrupulous. Buying used hardware helps increase the value of new hardware because buyers know that there will be a buyer for their surplus so that they don't have to pay to dispose of it. Even by buying a used Intel system, you helped out Intel. Full disclosure, I bought a fifty dollar C2D as well. I still have it, but I'm not using it. Maybe I'll give it away to someone who doesn't care about security, s
    1 hidden comment
  - **Re: (Score:2)**
    by drinkypoo (153816)
    Define old? Athlon XP has SSE but not SSE2, older Athlon has no SSE whatsoever. Neither can run Firefox, even 52 ESR or tor browser.
    Athlon 64 or X2 will do (or 64bit Sempron).
    Yeah, not that old. My backup system is a Phenom II X6 1045T, my backup to the backup is a Phenom II X3 720BE. IIRC the X6 has 8GB and the X3 has 4. I think I have one more motherboard with a relatively new dual-core, too, but that one might be flaky.
  - **Re: (Score:2)**
    by ArylAkamov (4036877)
    Shit sounds fucked where you are. Meet in person and stockpile hydrogen peroxide and acetone.
  - **Re: (Score:2)**
    by AHuxley (892839)
    Buy an older computer and find a supported OS for it.
  - **Re: (Score:2)**
    by Nite_Hawk (1304)
    Terribly sorry to hear about your situation. I hope things improve! FWIW, I think it's helpful to look at these issues (and really the the world in general) as a system of probabilities. Even absent these vulnerabilities your system is quite likely vulnerable to some other attack vector (as is mine, and as is basically every computer on the planet). It's just a question of how difficult is it to exploit and how likely is it that someone is going to do so.
    If you are truly worried that your government mig
- **Quick! Everyone panic! (Score:2, Interesting)**
  by GerryGilmore (663905)
  IMNSHO, the whole realm of Spectre/Meltdown vulnerabilities - while an interesting lab experiment - are complete horseshit. Consider:

  1) In order for ANY of these vulnerabilities to be useful, you MUST be running malware on your system. If so, you are already hosed.

  2) Given the enormous realms of malware extant than can much more quickly and easily grab your data (Hello, Equifax!), any true hacker would laugh at trying to use these vulnerabilities, because...

  3) The idea that malware can tickle the cache m
  6 hidden comments
- **Re:Quick! Everyone panic! (Score:5, Insightful)**
  by drinkypoo (153816) <martin.espinoza@gmail.com> on Saturday August 11, 2018 @07:24PM (#57109100)
  Homepage Journal
  IMNSHO, the whole realm of Spectre/Meltdown vulnerabilities - while an interesting lab experiment - are complete horseshit.
  Intel apologists are equally irrational to YHWH apologists.

In order for ANY of these vulnerabilities to be useful, you MUST be running malware on your system. If so, you are already hosed.
Javascript. Malware hidden in software. Virtualization. These are all real-world scenarios which affect basically everyone.
Given the enormous realms of malware extant than can much more quickly and easily grab your data (Hello, Equifax!), any true hacker would laugh at trying to use these vulnerabilities, because...
You're already vulnerable to shooting, so why worry about stabbing?
The idea that malware can tickle the cache millions of times to grab data (presuming it has not already been flushed), interpret said data and then prey that it is something useful, like passwords, when cache is normally filled with instructions more than data...
...has been demonstrated. Millions of times, so what? My computer does millions of things thousands of times per second.
Any of you who are now delaying purchases, etc. while you twist your hanky are doing the rest of us a favor by forcing prices down, so - Keep It Up!!
I'm not delaying purchases. I'm just happy I'm not using Intel, which is not only vulnerable to MELTDOWN, but is more vulnerable to SPECTRE-type attacks than my AMD CPU.

Reply to This Parent Share

twitter facebook linkedin
Flag as Inappropriate

- **Re: (Score:2)**
by GerryGilmore (663905)
"Intel apologists are equally irrational to YHWH apologists."
Considering that these vulnerabilities also (largely) apply to AMD and ARM, your cheap-shot snark is duly noted and ignored for the shit it is.
"Javascript. Malware hidden in software. Virtualization. These are all real-world scenarios which affect basically everyone."
Lots of word salad with no proof. Yawn...
"You're already vulnerable to shooting, so why worry about stabbing?"
That's a really stupid analogy, but let's pursue it for the fuck of it.

- **Re:Quick! Everyone panic! (Score:4, Informative)**
by drinkypoo (153816) <martin.espinoza@gmail.com> on Saturday August 11, 2018 @08:32PM (#57109378)
Homepage Journal
Considering that these vulnerabilities also (largely) apply to AMD and ARM, your cheap-shot snark is duly noted and ignored for the shit it is.
Mitigation is cheaper on AMD, because they at least tried to do the right thing. And they only tend to be a problem for 64-bit ARM. The biggest failures here are Intel and IBM.
Lots of word salad with no proof. Yawn...
There's no proof that those are real-world scenarios?
I can much more easily defend against a stabbing, because they need to be at very close range. (i.e. On your fucking system) whereas a bullet can travel over a mile and kill you.
Javascript is on your system. Malware hidden in applications is real, and on people's systems.
The rest of your statements are equally delusional and devoid of rationality, so...
...they're totally rational and you couldn't find any good arguments against them, either, so you just gave up.
Noted.

Reply to This Parent Share

twitter facebook linkedin
Flag as Inappropriate
1 hidden comment

- **Re: (Score:2)**
by ArylAkamov (4036877)
One damn good post.

- **Re: (Score:1)**
by GerryGilmore (663905)
"Mitigation is cheaper on AMD, because they at least tried to do the right thing. And they only tend to be a problem for 64-bit ARM. The biggest failures here are Intel and IBM."
OK, so everyone replace all of your Intel, 32-bit ARM and IBM CPUs immediately, because...

"There's no proof that those are real-world scenarios?"
Nope, none outside of lab conditions. Show me otherwise....I'm waiting....

"Javascript is on your system. Malware hidden in applications is real, and on people's systems."
Wait a minute! Th
2 hidden comments

- **Re: (Score:1)**
by Anonymous Coward
1) In order for ANY of these vulnerabilities to be useful, you MUST be running malware on your system. If so, you are already hosed.
Javascript is sufficient for many of these timing based attacks, even if it slows things down a little more. Proof of principle code already exists and show it can read quite a bit of browser memory in the time a person would reasonably spend on a page. I hope you're running NoScript and none of the sites you grant exceptions to ever get hacked...
1 hidden comment

- **Re: (Score:2, Informative)**
by Anonymous Coward
It sounds like you haven't read the details of these attack vectors.
1. The family of Spectre vulnerabilities are exploitable from javascript.
2. Yes, there is much malware, that doesn't make Spectre and meltdown attacks any less viable/devastating.
3. Statistical attacks have been used for a long time. Computers are great at performing them, because, yes, they are computers. Side channels don't need much bandwidth to steal critical information, like say, a users password or bank account details.
These att
2 hidden comments

- **That's what I thought too but no. That's all wrong (Score:2)**
by raymorris (2726007)
I thought the same thing, more or less, based on my understanding of basically how the low-level attack works. As it turns out, I was wrong. They have figured out how to use a "no big deal" issue to build an important and powerful attack around it. I got lost in the details and "couldn't see the forest for the trees", so to speak.
Others have pointed out "maleware running" could be JavaScript. Not even that is necessary, though - even sending specially crafted TCP packets to the target can do the trick! Goog
1 hidden comment

- **Re: (Score:1)**
by GerryGilmore (663905)
Well, when google is your technical authority, it's understandable that you'd be dead wrong...."even sending specially crafted TCP packets to the target can do the trick! Google Netspectre for details."

IF you actually READ TFA, you'll see that it REQUIRES a "gadget" (read: malware code) running on your fucking machine!! (I swear, the tech level on /. has descended to fucking Alex Jones level of paranoia - facts be damned!!) FFS!!

- **Gadgets are vulnerable OS components (Score:3)**
by raymorris (2726007)
The term "gadget", in this context, means vulnerable code, preferably OS code, an especially kernel code. That's pre-existing code, part of the OS, that's vulnerable.
For Netspectre, an interesting gadget is a network card driver that is vulnerable.
Gadget does NOT mean malware.

- **Re: (Score:1)**
by GerryGilmore (663905)
"For Netspectre, an interesting gadget is a network card driver that is vulnerable."
OK, show me one. Or, to be more exact (and I have written device drivers,BTW) show me a vulnerability worth its name that relies on ONE specific flaw in ONE specific NIC device driver, given the wide range of NIC drivers.
Sheesh! The lengths you guys will go to to defend the indefensible. (Indefensible, in this case, that the whole realm of SM panic is manifested by this weakest of arguments....)
1 hidden comment

- **Here are a couple of example gadgets. Bounds check (Score:2)**
by raymorris (2726007)
Here a couple of examples of Spectre gadgets. Suppose we have this code making sure the input doesn't try to access beyond the end of an array:
if (x array1_size)
y = array2[array1[x] * 4096];
Or maybe this code you might find in a firewall such as iptables. It checks to make sure the protocol of the packet is either TCP, udp, icmp, or another valid protocol:
if (packet.ethertype = maxtype) {
CurrentProt = EtherTypes[packet.ethertype];
}
Can you spot the problem?
1 hidden comment

- **The current network based has an important limit (Score:2)**
by raymorris (2726007)
The current network based variant has an important limitation in regards exfiltration rate. Based on past vulnerabilities and exploits, we can guesstimate that new developments might make it roughly 10X faster. That makes it even more interesting to use against chosen HTTPS sites to retrieve the private key.
The JavaScript based ones aren't currently the easiest way to build a botnet, but deploying such JavaScript on a site frequented by Lockheed Martin employees, or bank employees, could be really interesti

- **Nobody uses Intel gigabit NIC, right? (Score:2)**
by raymorris (2726007)
Here's the code for the driver uses with Intel network gigabit network cards. Hardly anyone ever uses that, right? Only people with Intel motherboards or Intel network cards, and other companies network cards that use the Intel chip.
https://github.com/torvalds/li... [github.com]
I see a couple hundred if statements in there. Maybe 20% of those will serve as a gadget. I bet you can find three or four bounds checks. In my other reply I showed you how to use a bounds check as a Spectre gadget.

- **She wrote upon it (Score:5)**
by TeknoHog (164938) on Saturday August 11, 2018 @07:08PM (#57109040) Homepage Journal

```
return to Spectre
address stack blown
go side channel
no safe zone
```

Reply to This Share

twitter facebook linkedin
Flag as Inappropriate

- **you forgot the ending... (Score:2)**
by Gravis Zero (934156)
Burma-Shave

- **THis goes back (Score:2)**
by jmccue (834797)
Well all of this goes back to what I have said to everyone I know, "Do nothing important in a WEB Browser". Which I get "It is safe and easy I do it all the time.
At least paying for a stamp to mail in a bill payment buys you protection that is lacking in WEB based tools. If your mail is tampered with, it is a crime. Granted the Gov my take a peek, but better than someone trying to drain your accounts.
The way things are going lynx is looking pretty good :)
1 hidden comment

- **Re: (Score:2)**
by HiThere (15173)
Well, it may not necessarily be safer, but I believe that at least it blocks attacks depending on Javascript.

- **Re: (Score:2)**

by drinkypoo (153816)
Granted the Gov my take a peek, but better than someone trying to drain your accounts.
The CA FTB decided I owed them money (I didn't) and drained my bank account. I filed for the back taxes and naturally I haven't heard from them since. They stole my money and I will never see it again. Assuming the government isn't going to steal from you is ridiculous.

Re: (Score:2)
by Nivag064 (904744)
What is the CA FTB?
Caribbean Associated Flying Transport Board???
1 hidden comment

It's too late (Score:2)
by AndyKron (937105)
Maybe it's too late. There was a chance back with the DOS, but not now. Computers are great but people are shit

by the time researchers find all the flaws in CPUs (Score:2)
by FudRucker (866063)
the only safe computers will be the ones completely disconnected from the internet, kept locked in a secure room where only authorized personnel are allowed to enter, i think its time for a completely new architecture built with security in mind from the ground up and the same goes for the software, no back doors, no remote code allowed to execute unless it is sandboxed and unable to touch the system
2 hidden comments

90 Days for Your New Chip (Score:2)
by mentil (1748130)
Manufacturers were notified of the weaknesses in May 2018 and were granted 90 days to remedy them before the results were published.
90 days may be the standard for Responsible Disclosure, but that's only reasonable for issuing a software patch. Intel doesn't issue new silicon to everyone affected within 90 days, it can take over a year before the next chips are available, and those might've had their design locked down well beyond that.

Stallman the Seer? (Score:1)
by Gerald Butler (3528265)
Richard Stallman clearly predicted this: https://en.wikipedia.org/wiki/... [wikipedia.org]

Related Links **Top of the: day, week, month.**
- 765 comments Developer Accidentally Deletes Three-Month of Work With Visual Studio Code
- 510 comments DOJ: Strong Encryption That We Don't Have Access To Is 'Unreasonable'
- 445 comments Should Developers Abandon Agile?
- 430 comments Equifax CEO Hired a Music Major as the Company's Chief Security Officer
- 416 comments 'Kernel Memory Leaking' Intel Processor Design Flaw Forces Linux, Windows Redesign

next

Theme Park Deploys Trained Crows To Collect Litter
136 comments

previous

Cryptocurrency Markets Lost $18 Billion Overnight
81 comments

Often statistics are used as a drunken man uses lampposts -- for support rather than illumination.