Subscribe to RSS

Follow me on Twitter

Join me on Facebook

Krebs on Security

In-depth security news and investigation

- About the Author
- Advertising/Speaking

05
Jan 18

Scary Chip Flaws Raise Spectre of Meltdown

Apple, Google, **Microsoft** and other tech giants have released updates for a pair of serious security flaws present in most modern computers, smartphones, tablets and mobile devices. Here's a brief rundown on the threat and what you can do to protect your devices.

At issue are two different vulnerabilities, dubbed "**Meltdown**" and "**Spectre**," that were independently discovered and reported by security researchers at **Cyberus Technology**, **Google**, and the **Graz University of Technology**. The details behind these bugs are extraordinarily technical, but a Web site established to help explain the vulnerabilities sums them up well enough:

> "These hardware bugs 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 Meltdown bug affects every Intel processor shipped since 1995 (with the exception of **Intel Itanium** and **Intel Atom** before 2013), although researchers said the flaw could impact other chip makers. Spectre is a far more wide-ranging and troublesome flaw, impacting desktops, laptops, cloud servers and smartphones from a variety of vendors. However, according to Google researchers, Spectre also is considerably more difficult to exploit.

In short, if it has a computer chip in it, it's likely affected by one or both of the flaws. For now, there don't appear to be any signs that attackers are exploiting either to steal data from users. But researchers warn that the weaknesses could be exploited via Javascript — meaning it might not be long before we see attacks that leverage the vulnerabilities being stitched into hacked or malicious Web sites.

Microsoft this week released emergency updates to address Meltdown and Spectre in its various Windows operating systems. But the software giant reports that the updates aren't playing nice with many antivirus products; the fix apparently is causing the dreaded "blue screen of death" (BSOD) for some antivirus users. In response, Microsoft has asked antivirus vendors who have updated their products to avoid the BSOD crash issue to install a special key in the Windows registry. That way, Windows Update can tell whether it's safe to download and install the patch.

But not all antivirus products have been able to do this yet, which means many Windows users likely will not be able to download this patch immediately. If you run Windows Update and it does not list a patch made available on Jan 3, 2018, it's likely your antivirus software is not yet compatible with this patch.

Google has issued updates to address the vulnerabilities on devices powered by its **Android** operating system. Meanwhile, **Apple** has said that *all* **iOS** and **Mac** systems are vulnerable to Meltdown and Spectre, and that it has already released "mitigations" in *iOS 11.2*, *macOS 10.13.2*, and *tvOS 11.2* to help defend against Meltdown. The Apple Watch is not impacted. Patches to address this flaw in Linux systems were released last month.

Many readers appear concerned about the potential performance impact that applying these fixes may have on their devices, but my sense is that most of these concerns are probably overblown for regular end users. Forgoing security fixes over possible performance concerns doesn't seem like a great idea considering the seriousness of these bugs. What's more, the good folks at benchmarking site **Tom's Hardware** say their preliminary tests indicate that there is "little to no performance regression in most desktop workloads" as a result of applying available fixes.

Meltdownattack.com has a full list of vendor advisories. The academic paper on Meltdown is here (PDF); the paper for Spectre can be found at this link (PDF). Additionally, Google has published a highly technical analysis of both attacks. Cyberus Technology has their own blog post about the threats.

Tags: apple, bsod, Cyberus Technology, google, Graz University of Technology, Intel, Meltdown, microsoft, SPECTRE

This entry was posted on Friday, January 5th, 2018 at 3:38 pm and is filed under The Coming Storm, Time to Patch. You can follow any comments to this entry through the RSS 2.0 feed. You can skip to the end and leave a comment. Pinging is currently not allowed.

27 comments

1. *Chuck*
   January 5, 2018 at 3:49 pm

   Thanks for the no nonsense reporting on this!

   Reply
2. *Petepall*
   January 5, 2018 at 3:51 pm

   Nice Headline!

   Reply
3. *James Cameron*
   January 5, 2018 at 3:52 pm

   > Google has issued updates to address the vulnerabilities on devices powered by its Android operating system

   Not on my phone, a Pixel XL.

   Reply

   - *Irve Towers*
     January 5, 2018 at 5:05 pm

     Monthly updates included fixes for Pixel XL Posted 1/3/2018.. Got the update on my Pixel XL.

     Reply
4. *Tammy*
   January 5, 2018 at 3:55 pm

   Ha, good play on words for the headline Brian! i feel you and others may be rather busy 2018, hell of a start to the year.

   Reply
5. *Gary*
   January 5, 2018 at 4:09 pm

   Thanks for putting this into plain english. The technical aspect for Spectre is mind blowing.

Reply

6. *Arbee*
   January 5, 2018 at 4:15 pm

   I wrangle a few machines, all running W-7 (SP-1); one has an AMD processor; the others have some flavor of Intel.

   Patch Tuesday arrived early this month. All my machines are set to “check for updates but let me choose whether to download and install them”. On a typical Patch Tuesday, I don’t rush to be at the head of the line, but I’m usually in the queue before Microsoft alerts me. KB4056894 knocked on my door mid-morning Fri 5 Jan.

   KB4056894 conflicts with certain anti-virus products, as mentioned in the story. This link

   https://docs.google.com/spreadsheets/d/184wcDt9I9TUNFFbsAVLpzAtckQxYiuirADzf3cL42FQ/htmlview?sle=true#gid=0

   offers a partial list of anti-virus products and their compatibility with KB4056894. “Partial list”: for example, the list includes Microsoft’s “Windows Defender” but not Microsoft Security Essentials.

   Bottom line: To properly install KB4056894, a specific registry entry is required. Details under “Known issues…”

   https://support.microsoft.com/en-us/help/4056894/windows-7-update-kb4056894

   My experience: no problem with the update installation, though the required restart took a few minutes more than typical.

   Intel-related resources:

   Intel firmware updates advisory page: https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086&languageid=en-fr

   Intel-SA-00086 Detection Tool: https://downloadcenter.intel.com/download/27150?v=t

   Reply

   - *George G*
     January 5, 2018 at 8:19 pm

     Arbee, thanks for the spreadsheet.

     It does not list AVG.
     This is from AVG support website:
     “Hi guys,

     AVG 2017 is compatible with the Windows patch and we protect against the malware since December 2017 and it is storing the required keys into the registry since Jan 3rd, 2018.

     Regards,
     Bhuvana, AVG Customer Care.”

     However, I find that the last Windows update on my desktop (W7) was on Dec. 14.

     Reply

     - *George G*
       January 5, 2018 at 9:17 pm

       AVG (the program, not its database) had to be updated.
       After that Windows uodate did show up.

       Reply

7. *KathyB*
   January 5, 2018 at 4:17 pm

   I use ESET as my AV. Both of my Windows 10 PCs had the patch applied and I’ve notice no change in performance.

   Reply

8. *Tammy*
   January 5, 2018 at 4:19 pm

Anyone know if these chip problems could screw with your router, now that would be very scary.

Reply

- *Matt*
  January 5, 2018 at 4:30 pm

  That’s what I was going to ask… Scary for a lot of people if it dawn be used to defeat firewalls. Any comments from networking hardware makers?

  Reply

9. *Charles Dennett*
   January 5, 2018 at 4:20 pm

   What about older Android devices for which google no longer issues OS updates or security patches like my Nexus 6 phone and even older nexus 7 tablet? Everything I’ve read so far mentions supported devices and these are no longer supported.

   Reply

   - *Joe*
     January 5, 2018 at 4:49 pm

     Even though Google no longer provides updates for old devices like the Nexus 7, you can install LineageOS. I have LineageOS 14.1 (Android 7.1.2) on my Nexus 7, and the LineageOS people apply the latest security patches.

     Reply

10. *Geoff*
    January 5, 2018 at 4:22 pm

    Great summary as usual. Looking forward to hearing if POC attack code for these vulns starts getting incorporated into any widely distributed malware.

    Reply

11. *DaaBoss*
    January 5, 2018 at 4:30 pm

    Still on Android 5.0 or lower??

    Call your cell phone provider and ask for the updates. It’s high time we demanded the ability to easily update our OS, using T-Mobile, Cingular, Sprint, etc.

    Orphaning older phones is no longer acceptable. A five year life of OS updates should be the bare minimum we should expect, or demand a rebate or partial refund.

    If providers won’t keep us updated, then let’s demand them from the hardware vendors like Samsung, or buy a different brand.

    Reply

12. *Tammy*
    January 5, 2018 at 4:40 pm

    Also will it screw with any xp and their embedded systems! it gets worse the more i think.

    Reply

13. *IRS iTunes Card*
    January 5, 2018 at 4:50 pm

    Researchers keep issuing high profile warnings about genuinely dangerous new security flaws, and a few weeks or even days later they are all but gone.

    Sooner or later people are going to start questioning the credibility of the research and the seriousness of the situation.

    Reply

14. *Dave*
    [January 5, 2018 at 4:54 pm]

    I also just want to thank you for your reporting on this subject. Clear, precise and easy to understand.

    Reply

15. *tom*
    [January 5, 2018 at 5:00 pm]

    Thank you Brian for all your hard work to keep us informed; great summary on present crisis.

    Reply

16. *Brook S.E. Schoenfield*
    [January 5, 2018 at 5:33 pm]

    You might mention that in order to exploit, an attacker has to get the exploit code onto a device. Javascript certainly makes that considerably easier. Still, safe computing practices do provide some bar to exploitation.

    Reply

17. *Alan*
    [January 5, 2018 at 5:50 pm]

    It amazes me, as MS makes billions, the end user is the one who pays for all their vulnerabilities while they have very little accountability.

    Reply

    - *Larry*
      [January 5, 2018 at 9:31 pm]

      So true!

      Reply

18. *vb*
    [January 5, 2018 at 6:16 pm]

    From what I've read, the exploits for these vulnerabilities are not easy to implement. I think that government agency hackers will have and use these vulnerabilities in their exploit tools. But I doubt that these exploits show up in consumer-targeted malware.

    Most systems with shared processing and memory (cloud computing) are managed by professionals and will be patched long before exploit code is written.

    Reply

19. *Catwhisperer*
    [January 5, 2018 at 9:56 pm]

    As somebody who remembers the days of bit-slice, this appears to be a problem in the underlying architecture. I've downloaded both white papers, but haven't had time to read them in depth yet. They are intense…

    But if it's a problem in the predictive branching and execution part of the microcode, it's going to take hardware replacement or microcode updating (which does work). But that ability to update the microcode also much depends on processor model and motherboard model. Tough nut to crack at the transistor/microcode level, IMHO…

    Reply

20. *IRS iTunes Card*
    [January 5, 2018 at 10:41 pm]

    Spectre & Meltdown – Computerphile video
    https://www.youtube.com/attribution_link?a=B1yiaKFH4i70cxMY&u=/watch%3Fv%3DI5mRwzVvFGE%26feature%3Dem-uploademail

Reply

21. *Tom Mix*
January 5, 2018 at 11:55 pm

Is there any vulnerability with smart DVD players and TV's, cable modems and/or networking boxes such as Airport Extreme? If so, how will they be patched?

Reply

Leave a comment

Name (required)

Email (required)

Website

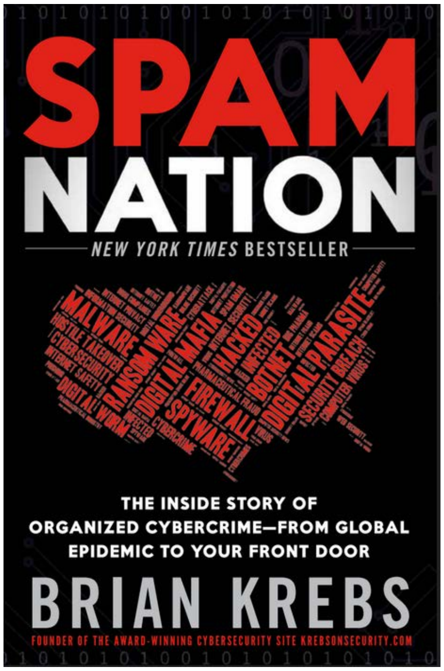
Comment

Submit Comment

- **Mailing List**

  Subscribe here

- **Have a Look at My Book!**

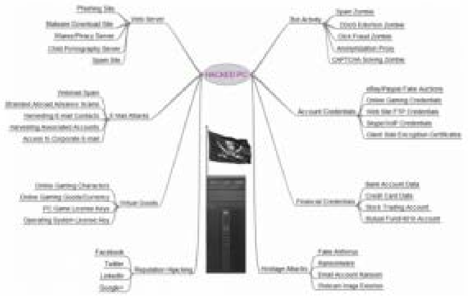

SPAM
NATION
NEW YORK TIMES BESTSELLER
THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR
BRIAN KREBS
FOUNDER OF THE AWARD-WINNING CYBERSECURITY SITE KREBSONSECURITY.COM

A New York Times Bestseller!

- Buy at Amazon
- Donate with PayPal
- ## Recent Posts
  - Scary Chip Flaws Raise Spectre of Meltdown
  - Serial Swatter “SWAuTistic” Bragged He Hit 100 Schools, 10 Homes
  - Kansas Man Killed In ‘SWATting’ Attack
  - Happy 8th Birthday, KrebsOnSecurity!
  - 4 Years After Target, the Little Guy is the Target
-
- ## All About Skimmers

Click image for my skimmer series.

- ## The Value of a Hacked PC



Badguy uses for your PC

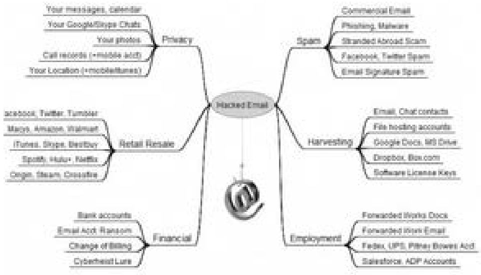
- ## Tools for a Safer PC

Tools for a Safer PC

- ## The Pharma Wars

Spammers Duke it Out

- ## Badguy Uses for Your Email



Your email account may be worth far more than you imagine.

-

eBanking Best Practices

eBanking Best Practices for Businesses

- ## Most Popular Posts
  - Online Cheating Site AshleyMadison Hacked (798)
  - Sources: Target Investigating Data Breach (620)
  - Cards Stolen in Target Breach Flood Underground Markets (445)
  - Reports: Liberty Reserve Founder Arrested, Site Shuttered (416)
  - Was the Ashley Madison Database Leaked? (376)
  - True Goodbye: 'Using TrueCrypt Is Not Secure' (363)
  - Who Hacked Ashley Madison? (361)
  - Following the Money, ePassporte Edition (353)
  - U.S. Government Seizes LibertyReserve.com (315)
  - Extortionists Target Ashley Madison Users (310)
- ## Category: Web Fraud 2.0

Innovations from the Underground

-

  ID Protection Services Examined

- **Is Antivirus Dead?**

Dedicated, VPS/VDS, Shared Hosting Domains, SSL Certificates
Долгосрочное сотрудничество работаем более 2х лет
от 2000$ в месяц
Вы сами выбираете количество и порядок серверов в маршруте
EXECRYPT
5000$ в месяц
ТРЕБУЮТСЯ КРИПТОРЫ с постоянной поддержкой
SOLLHOST ABUSE"IMMUNITY HOSTING SERVICE
Новое слово в криптовании

  The reasons for its decline

- **The Growing Tax Fraud Menace**

  File 'em Before the Bad Guys Can

- **Inside a Carding Shop**

A crash course in carding.

Beware Social Security Fraud

my Social Security– Sign In Or Create An Account

my Social Security

At each stage of your life, my Social Security is for you. Your personal online my Social Security account is a valuable source of information beginning in your working years and continuing throughout the time you receive Social Security benefits.

If you receive benefits or have Medicare, you can:

Use a my Social Security online account to:

- Get your benefit verification letter;
- Check your benefit and payment information and your earnings record;
- Change your address and phone number; and
- Start or change direct deposit of your benefit payment.

Sign up, or Be Signed Up!

How Was Your Card Stolen?

Finding out is not so easy.

Krebs’s 3 Rules…

…For Online Safety.