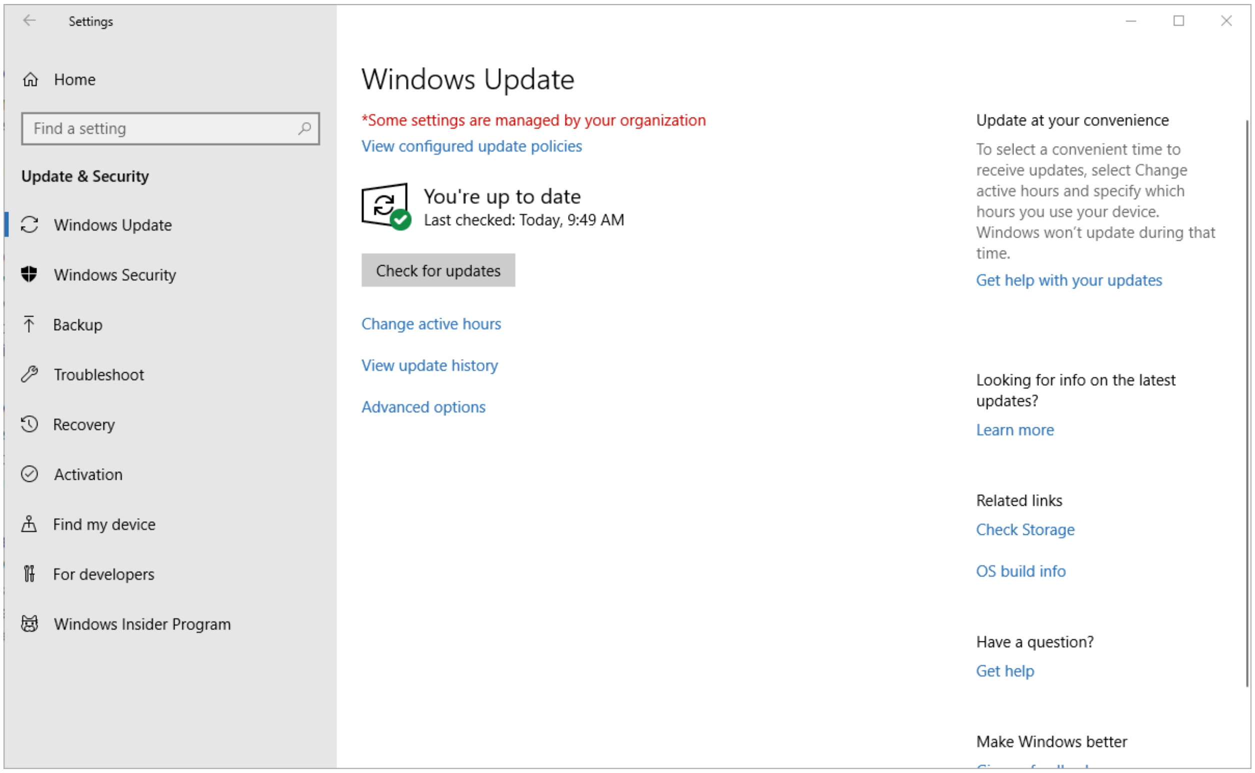
# What I did in Response to the Presentation by Eric Moore on March 10, 2018
# By Ron Mettler, March 12, 2018

My one year old home assembled computer never coughed up as far as I can tell due to a virus, ransomware, malware or any other threat. So I took Eric's advice anyway to help avoid problems with the Spectre and Meltdown vulnerabilities to make sure all of my system software was up to date. I use Windows 10 Professional 64 bit operating system with Microsoft Office 2016 suite and various other applications. I made sure that I had the latest version of Windows 10 by clicking Start, Settings, Update & Security, then Check for updates. There were no new updates missing as indicated in the below figure:



Windows Update

*Some settings are managed by your organization

View configured update policies

You're up to date

Last checked: Today, 9:49 AM

Update at your convenience

To select a convenient time to receive updates, select Change active hours and specify which hours you use your device. Windows won't update during that time.

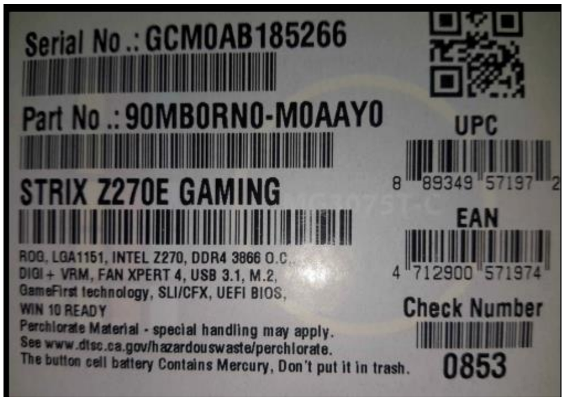
Looking for info on the latest updates?

Related links

Have a question?

Make Windows better

I then checked the motherboard manufacturer's site to determine which BIOS update was the latest and also the other newer versions of drivers. My motherboard is an ASUS Z270E with an Intel i7-7700K CPU:



Serial No.: GCM0AB185266

Part No.: 90MB0RN0-M0AAY0

STRIX Z270E GAMING

ROG, LGA1151, INTEL Z270, DDR4 3866 O.C.,
DIGI+ VRM, FAN XPERT 4, USB 3.1, M.2,
GameFirst technology, SLI/CFX, UEFI BIOS,
WIN 10 READY
Perchlorate Material - special handling may apply.
See www.dtsc.ca.gov/hazardouswaste/perchlorate.
The button cell battery Contains Mercury, Don't put it in trash.

UPC

8 89349 57197 2

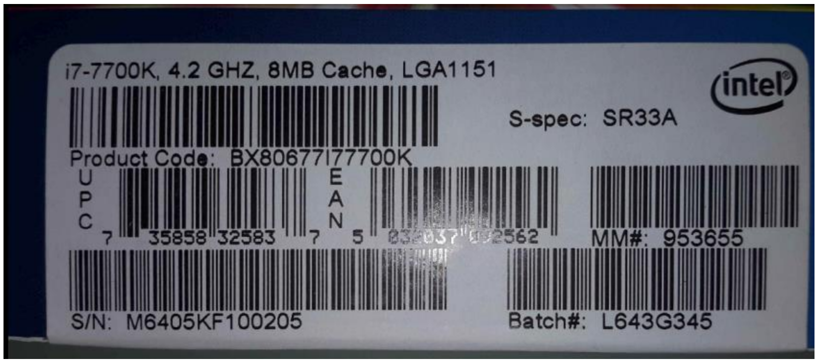
EAN

4 712900 571974

Check Number

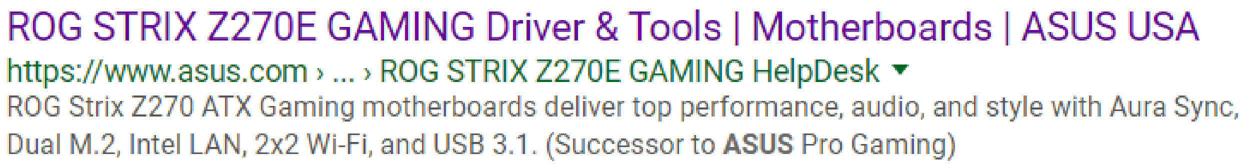
0853

**Motherboard**



**CPU**

My Google search for drivers used “asus z270e drivers” resulted in the following item:



ROG STRIX Z270E GAMING Driver & Tools | Motherboards | ASUS USA

https://www.asus.com › ... › ROG STRIX Z270E GAMING HelpDesk ▾

ROG Strix Z270 ATX Gaming motherboards deliver top performance, audio, and style with Aura Sync, Dual M.2, Intel LAN, 2x2 Wi-Fi, and USB 3.1. (Successor to **ASUS** Pro Gaming)

Clicking on the link took me to a screen that required that I select my OS which then listed the available drivers and BIOS updates as follows:

VGA

**Version 23.20.16.48492017/12/28307.62 MBytes**

Intel Graphics Accelerator Driver

Improve system stability & Support Windows 10 latest version (Build 16299)

BIOS

**Version 12032018/01/097.77 MBytes**

STRIX Z270E GAMING BIOS 1203

Improved DRAM compatibility.

Fixed SAMSUNG M.2 device issue.

Fixed SanDisk M.2 device issue.

Fixed AMD SSD device issue.

Fixed SteelSeries Keyboard issue.

Update CPU MicroCode.

AUDIO

**Version 6.0.1.82732017/12/26751.18 MBytes**

Realtek Audio Driver V6.0.1.8273

LAN

**Version 22.92017/12/26250.93 MBytes**

Intel LAN 22.9

## Wireless

### Version 12.0.0.4482017/12/0641.7 MBytes

Wi-Fi Driver
Wi-Fi Driver V12.0.0.448 for Windows 10 64bit.(WHQL)

## BIOS-Utilities

### Version -2017/03/31195.32 KBytes

BRenamerl
How to use:
1.Extract both BRenamer and BIOS image file into the folder of your preference.
2.Execute Brenamer.exe
3.Brenamer will change all BIOS image file into the correct file name ready for USB BIOS Flashback and Crashfree BIOS 3 to use

## Chipset

### Version 11.7.0.10452017/12/2679.47 MBytes

Intel ME V11.7.0.1045

## SATA

### Version 15.9.0.10152017/12/2621.4 MBytes

IRST V15.9.0.1015

## BlueTooth

### Version 10.0.0.3092017/07/2458.54 MBytes

ASUS Bluetooth Driver
Improve system stability & Support Windows 10 latest version.

I downloaded the files for the "VGA, BIOS, Audio, Lan, Wireless, Chipset, SATA, and Bluetooth". The Utilities, BIOS Utilities, Qualified Vendor List and Declaration of Conformity were items that did not appear to be relevant. All of the files were .ZIP files so I had to extract the contents of each file. Click on the ZIP file, then on "Extract All": A folder is then created with all of the files needed for the updated driver. For my drivers each folder contained a file titled "ASUSSetup.exe" I clicked on that file and the driver was updated. Each of the other downloaded ZIP files were processed in the same manner except for the BIOS file.

Updating a BIOS is a process that is unique for the particular manufacturer of the motherboard. My BIS update file was called "STRIX-Z270E-GAMING-ASUS-1203.CAP". In order to use that file for updating the BIOS required that I go into the BIOS, then in the Advanced section I located a BIOS update utility. During the process of running that utility, I was asked for the location of the BIOS update file. I had to navigate to my drive and fid the unzipped file and select it. The BIOS utility took a couple of minutes to run and complete the update. At least for my system, a reboot then completed the required updates. I had already checked all of my other applications for updates.

Each computer will have some similar set of routines in order to find and update the needed drivers and BIOS files.
For **Dell computers** go to http://www.dell.com/support/home/us/en/19?c=us&l=en&~ck=mn , type in the Service Tag number found on the stick on decal that is on the case.
For HP computers go to https://support.hp.com/us-en/drivers enter the data to identify your computer.
For ACER computers go to https://www.acer.com/ac/en/US/content/support enter the data to identify your computer.

The following article appeared in a Blog that I subscribe to. In reading the article, I have come to the conclusion that the Spectre and Meltdown issues border on fake news.

## Spectre and Meltdown: What's Left after Everyone Panicked for a Moment?

By Patrick Gebhardt, Feb 26, 2018

All these Spectre and Meltdown security risks remind me of Bill Maher jokes: you don't know if you get them, but at least you know you're not laughing. Maybe it's not as dangerous as everyone thinks. Or maybe it is? What we do know is that there are now almost 140 different malware samples trying to exploit the Meltdown and Spectre processor gaps. It's hard to determine whether this has led to concrete attacks on users; however, it is highly probable that there haven't been any such attacks. Also, we know the history of the whole mess, but what don't we know? Everything else.

Almost 2 months after everyone with a keyboard and fingers told the internet about their fears of Spectre and Meltdown, the majority of hardware manufacturers and security researchers are still working on the issue. While manufacturers, including Intel, are busy developing and delivering patches, security researchers of all kinds are already writing malware exploits. The fact that not everything is running according to plan with these attempts also fits into the picture. Intel is currently being sued by more than 30 groups for the Meltdown and Spectre vulnerabilities but instead of resolving the security gaps and clarifying them, Intel created additional chaos at the end of January. Because updates on certain older computers led to crashes or unnecessary restarts, the chip giant now advises against installation. Meanwhile, other PC manufacturers had already processed Intel's rework attempts to BIOS updates. And many of these vendors are now taking down the updates from their websites again. There are also several Linux distributions that are withdrawing their fixes.

More and More Malware, but Real Attacks Are Unknown

The nearly 140 different malware versions, which are supposed to attack the gaps, are based on the known proof-of-concept code and target Windows, macOS and Linux. They come from security researchers, so they were probably written for testing purposes, or they come from anti-virus vendors who, in turn, received them from their customers. The great number of samples is explained by the fact that the malware or exploit writers are already busy determining whether the gaps can somehow be exploited to steal data. Realistically, you can only expect an attack via a browser, at least for now. Users should therefore always keep their browser software up to date. Other methods of attack seem to be too complex, and therefore too cost-intensive, for the less resourceful writers of malware.

## What Constitutes a Crime?

So I ask myself: what are we talking about here? A potential danger? Well... alright. An attack on end users and businesses? Not for the time being. Based on our current knowledge, there is no evidence of concrete attacks on users. The firewall manufacturer Fortinet, which has been alerting its users to the danger, apparently has no concrete evidence of attacks. The company also makes no mention of foiled attacks on customers, nor are we aware of any authentic emails with malicious code attachments that would have been sent to victims and that exploit Meltdown or Spectre gaps for attacks.

## Make Sure Your OS Is Up to Date

Intel is now expanding its Bug Bounty Program to detect and eliminate security vulnerabilities sooner. From now on, the so-called Side Channel Vulnerabilities will be announced until the end of the year with a reward of 250,000 US dollars, all other found bugs or exploits will be rewarded with up to 100,000 US dollars. In addition to the increased premiums, the program is also set much more openly. However, Spectre and Meltdown have once again made it clear how painful the technical dependence on a few suppliers can be. So what are we left with? Same advice as a few weeks ago: keep your operating system and your browser up to date. This is the best approach to combatting the phenomenon of Meltdown and Spectre; if anything changes, you will hear from us immediately (and subscribing to our blog would be another smart move). Also, your PRTGinstallation will run as smoothly as always if you make sure your operating system has all the latest security patches installed.