ArchivistaBox 2018/I: Safety from a single source

Egg, 18th Janaury 2018: *Almost on time for the New Year, security problems appeared with almost all processors. This blog comments on the problems and also offers basic thoughts on current systems and related security issues. And of course the ArchivistaBox 2018/I is a first remedy.*



Meltdown and Spectre: A misfortune rarely comes alone

Before the first working day on January 3, 2018, **media reports** appeared that all current CPU processors would have massive security gaps. The names Meltdown and Spectre-1 and Spectre-2 made the rounds. All Intel computers are currently affected by Meltdown, with the two Spectre variants almost all CPUs (Intel/AMD and ARM) being vulnerable to attacks.

What's this about? To put it simply, a program can read any data from another program and thus (as long as confidential data is stored in plain text)"spits out" this information (against all protection mechanisms) at will. The problems have arisen over more than a decade, because the speed of the computers has been continuously increased without thinking about security.

Since 2005, the ArchivistaBox (against any other trend) has been following the path of resource conservation at every conceivable point. Nowadays, the ArchivistaBox can be operated without any problems on the microcomputer Raspberry PI (Albis and Bachtel) — and funny enough, these computers are not affected by the attacks.

Due to the fact that ArchivistaBox ships a box appliance (hardware and software unit) with the ArchivistaBox, it is unavoidable that the development of the ArchivistaBox requires a very thorough examination of the operating system. Over the last few years it has been observed that, in our opinion, the development has been taking place for some time now, in terms of innovation rather than stability.

Here are two (non-final) examples: In August 2015, **ARM-based ArchivistaBoxes** were presented, setting new standards in terms of both power consumption and space requirements. These were barely noticed on the market. Intel or AMD, everything else seems to be too much of a foreign word in the server market to be of interest. In September 2016 an **updated base with Debian Jessie** was released. The all-embracing' milling' boot service SystemD was not built into the startup process.



These and many other measures mean that ArchivistaBox is slimmer and much more performant than other comparable systems. Customers are constantly amazed at the moderate hardware on which ArchivistaBox is delivered. But with the approach of being' stingy' about hardware, with this approach ArchivistaBox is the exception, certainly not the rule. This applies to business software (here the ArchivistaBox offers an alternative), but unfortunately also increasingly for Linux itself. The days when Linux could be described as slim are over. Today, the Linux kernel requires well over 10 GByte before it can be compiled from the program code to the desired hardware.

In order for all this work to be completed within reasonable time, up-to-date hardware is necessary. But that is precisely where the problem lies. The performance of current hardware can only be improved to the desired extent by creating caches. The processor, for example, calculates things which he presumably assumes will be needed later so that he can access these parts (possibly faster) later on.

The current problems of Meltdown and Spectre are now buried in the fact that hardware

manufacturers have barely or obviously not given enough thought to how the cached data can be protected against access by other programs. And that's why almost all processors are vulnerable today. It is currently impossible to predict where the journey will take us. It is clear that in the future it will not only be about how fast a hardware is, but above all about how secure it is.

ArchivistaBox 2018/I with current patches available

In the last two weeks, there has been an intensive analysis of Meltdown and Spectre. On the positive side, it should be noted that ArchivistaBox is not actually affected by Meltdown because almost all systems are delivered with AMD and/or ARM. The situation with the Spectre-1 and Spectre-2 is less good. Almost all ArchivistaBoxes (except Albis and Bachtel) are affected. Until yesterday there were no patches for Spectre-1 and Spectre-2. Now that the first patches are available, they have of course been integrated into ArchivistaBox 2018/I.

```
# cat /proc/version
Linux version 4.9.77 (root@avbox177) (gcc version 8.0.1 20180118
(experimental) (GCC) ) #1 SMP Thu Jan 18 14:01:21 CET 2018

# cat /sys/devices/system/cpu/vulnerabilities/meltdown
Mitigation: PTI

# cat /sys/devices/system/cpu/vulnerabilities/spectre_v1
Vulnerable

# cat /sys/devices/system/cpu/vulnerabilities/spectre_v2
Mitigation: Full generic retpoline
```

Current status (18.1.2018): Meltdown and Spectre-2 can be fixed, at present there is no protection for Spectre-1. Because the Spectre patches require software that has not yet been tested in all corners and ends (GCC compiler with version 8.0.1 is described as experimental), the corresponding fixes (Kernel 4.9.77) are only delivered for those customers who wish to do so. This is clear from the point of view that Spectre-1 and Spectre-2 require an attack locally and that practically no customer works locally on the ArchivistaBox. There are currently no known exploits via web services, and corresponding attacks (JavaScript) would also have to be carried out on computers that access the ArchivistaBox.



In this sense, the desktop computers should be patched first and foremost. It remains to be seen whether and to what extent this is possible with smartphones. Apple is likely to be in a much better position here, because the hardware used is modest compared to Android. Although patches are currently available at Android, it is far from clear whether and how the manufacturers integrate or deliver them.

The ArchivistaBox systems themselves are updated by the customers via WebConfig. If you would like to receive an update, please let us know and the corresponding release will be made available (free of charge within the scope of the maintenance contract). Questions about security issues concerning Meltdown and Spectre are gladly answered by **e-mail** or **telephone.**

Update from 19.2.2018: In the meantime kernel 4.9.82 is included. For the first time there is a protection against (certain) attacks on Spectre-1.

Picture sources: Hiking between Florence and Siena, turn of the year 2017/18, https://azurgo.ch