Error on CPU seriously affects cloud storage services

Cloud patching platforms are very fast, but the hardest part is still there.

This article is in the series: Overview of vulnerabilities on Intel, AMD, ARM chips: Meltdown and Specter. Please read all the articles in the series to get information as well as take steps to protect your device against these two serious security holes.

This week, the technology world was excited when two security holes were discovered on Intel, AMD and ARM chips, named Meltdown and Specter. AMD and ARM both warned of security flaws like Intel processors. While Meltdown is 'shallower' and even the PoC describes how to exploit, Specter is 'deeper', more difficult to patch and 'promising' the possibility of being exploited for years to come.

Everyone is worried about personal devices with emergency patches to protect the device, but many experts say the more serious damage is when they are exploited on cloud services.

1. Windows 10 KB4056892 emergency update (build 16299.192)
2. Microsoft released an update for Surface, protecting it from Meltdown and Specter

"These vulnerabilities will allow a person to see the data of another co-host," said Mounir Hahad, chief threat research officer at Juniper Networkks. 'That's why many organizations avoid using host services with sensitive information.'

Both Meltdown and Specter are related to data leakage, so it is more serious when a device is shared with many users. By attacking commands that run in parallel with the correct time, an attacker can retrieve data from the cache, low-level processes such as web plugins, then get passwords or sensitive data. other.

Along with server sharing, cloud services are more vulnerable to exploitation

On personal computers, the most useful way for an attacker is to use privileged escalation techniques, low-level malware uses Specter to control the computer. But there are many ways to take control of the machine and once you've got your foot in, you don't know how to attack.

But privileged escalation will be very scary on the cloud, where the server works with many people at the same time. Amazon Web Services and Google Cloud allow sharing a program on thousands of servers located in data centers around the world. The parties share the hardware as well as many people on a plane trip.

Using such hardware does not have security issues because even though many people use it on one server, they have different software versions, cannot jump from one side to the other. But Specter can change that, allowing an attacker to steal data from anyone who shares the same chip.

Cloud services are also very attractive to those who want to make money from Specter. Many medium-sized businesses run their entire architecture on AWS or Google Cloud, trusting to put sensitive information on it. Trading Bitcoin, chat applications, even government agencies, keeps passwords and sensitive information on the cloud server. If you run the web service, there is no other way. If exploited, do not know what data will be stolen.

Until now, cloud platforms all recognize this very seriously and find ways to protect it. Amazon Web Services, Google Cloud and Microsoft Azure immediately released the patch, although there is no evidence that it is possible to exploit these holes in the cloud.

If you're still hesitant, it's because they have to wait for patches from third parties, such as Amazon EC2, for example. Great services are fast to handle, so we can hope there will be no catastrophe in the short term.

The worry is that in a few years, deep root holes like Specter will be very difficult to destroy. Researchers will find new variants - as seen with the Stagefright disaster - and not always as widely available as Specter and Meltdown. It's not hard to imagine that in the next few months, an undiscovered vulnerability has fallen into the wrong hands, and then AWS or Google Cloud will be in sight.

It may not be dangerous immediately but the long-term consequences are difficult to say

This will be a nightmare because the above platforms are under almost everything we use on the Internet, running applications on the phone, streaming music . It's hard to say if any part of the Internet doesn't go through This server is at some point.

Understandably, it is the Internet. And despite being handled by the best security groups in the world, attacks are almost limitless. The handling of Specter 's consequences will be one of the most difficult things security systems face - and this problem will not be resolved overnight.

(When asked, the Google representative said that their cloud service was protected from Meltdown and Specter even without details. Amazon did not comment.)

Below is a patch guide from cloud platforms.

1. Amazon Web Services *https://aws.amazon.com/de/security/security-bulletins/AWS-2018-013/*
2. Google Cloud *https://support.google.com/faqs/answer/7622138*
3. Microsoft Azure *https://azure.microsoft.com/en-us/blog/securing-azure-customers-from-cpu-vulnerability/?ranMID=24542&ranEAID=nOD/rLJHOac&ranSiteID=nOD_rLJHOac-Rrfhv5WdBAfXXcPsFXluFw&tduid=(de4f40b167ccb67d4b9e76ff50c58d3b9e76ff50c58d3b9e76ff50c58d3b9e76ff50c58d3b9e76ff50c58d3b9e76ff50c5(256380) (256380) (2459594) (nOD_rLJHOac-Rrfhv5WdBAfXXcPsFXluFw) ()*

See more:

1. How to protect the computer against Meltdown vulnerability on CPU?
2. Multicloud - a new step in cloud computing technology
3. AWS and Azure dominate the cloud world, above all, no one wins