PortSmash - New vulnerability on multi-threaded CPU

Researchers think this is a serious error, but Intel does not.

PortSmash is a dangerous side channel vulnerability, exploiting active streams simultaneously to steal the key and determine what the processor is doing. Currently, this vulnerability has been confirmed on the Kaby Lake and Skylake chiP but it is also possible to work on AMD's ultra-high-end processors.

SMT (Simultaneous multi-threading) creates two logical cores on each physical core, but these two cores can see what the other thread is doing.

Malware exploiting the PortSmash vulnerability will operate on a parallel logical core to target the target process and legitimize it. It will then record all data leaking from the legal process - usually the operating time - and then reconstruct what the other core is doing. It is supposed to steal a lot of information, most effectively evaluating cryptographic keys because of how the processor calculates them.

A similar flaw using SMT as a weakness is TLBleed, announced in June. It can identify a 356-bit encryption key for more than 17 seconds, using only 2 milliseconds of data. PortSmash may (or may not) be slower, but the possibility is that it will be more flexible.

'PortSmash is very flexible and there are few prerequisites, it does not need to know about cache connections (connecting from main memory to cache), machine learning techniques or reverse engineering. PortSmash also doesn't need root access, 'said Billy Bob Brumley, a researcher with PortSmash.

Brumley and his team consisted of four other researchers from universities in Cuba and Finland saying that the server architecture would be most affected. 'I think remote login scenarios are the biggest threat.' For example, when malicious users log into the website, they can use PortSmash to discover the encryption key used by the website and then hack the server to steal the data.

PortSmash can steal encryption keys

However, there is no need to panic. OpenSSL, a widely used encrypted library on the Internet (more than 60%) has just released a patch to prevent access via this direct method. They also said the general patch will soon be released, but security researchers say the hardware or BIOS also needs to take action.

They announced the vulnerability to Intel on October 1, but Intel did not agree, saying that encrypted libraries such as OpenSSL must prevent these security flaws themselves. AMD is considering its role in this regard.

On GitHub, there is also PoC if you want to try using PortSmash, it can steal the private key P-384 OpenSSL from TLS server running OpenSSl software which has not been upgraded to version 1.1.1

See more:

1. Updating Windows 10 in the future will help the machine run faster by patching Specter
2. Foreshadow - the fifth most serious security hole in the CPU in 2018
3. Serious security vulnerability on Intel chips