Specter V2 vulnerability re-appears to attack Intel, Arm CPUs, AMD chips are not affected

Security research team VUSec and Intel have just released a notice of a dangerous remote execution vulnerability of the Specter class, known as Branch History Injection or BHI.

The vulnerability affects all Intel processor models released in the past few years, along with certain Arm processor cores. The specific list of affected products is unknown, but will certainly include Intel's newly-launched 12th Gen Alder Lake CPU family. Surprisingly, AMD chips don't seem to be affected by this vulnerability, at least for now.

BHI is essentially a proof-of-concept attack that affects CPUs that are already vulnerable to Specter V2 exploits, but with all mitigations in place. As reported by Phoronix experts, this new mining method can bypass Intel's eIBRS and Arm's CSV2. BHI re-enables cross-privileged Specter-v2 mining, enabling kernel-to-kernel (aka BTI in internal mode) mining and paving the way for malicious actors to inject prediction entries into History Injection to leak kernel data. As a result, arbitrary kernel memory on targeted CPUs could leak, potentially revealing confidential information, including passwords.

To prove their claims, the researchers also released a proof of concept (PoC) document, which shows the state of an arbitrary kernel memory leak, revealing the original hashed password of a vulnerable system. attack.

Preliminary investigation shows that all Intel processors starting with Haswell (released in 2013) extending to the latest Ice Lake-SP and Alder Lake are affected by the security vulnerability mentioned above. above. However, Intel says the company is about to release a software patch to mitigate this problem.

Besides, many core architectures from Arm, including Cortex A15, A57, A72 as well as Neoverse V1, N1 and N2 are also affected. Arm is expected to release a fix patch in the near future. It is not clear at this time whether custom versions of these cores (e.g. select cores from Qualcomm) will be affected, and when potential security vulnerabilities will be addressed.

Since this is a proof-of-concept vulnerability and is being worked on by Intel and Arm, it cannot be exploited to attack a client or server right now - as long as all the latest patches are installed. full. There is no indication that the mitigations will affect processor performance.