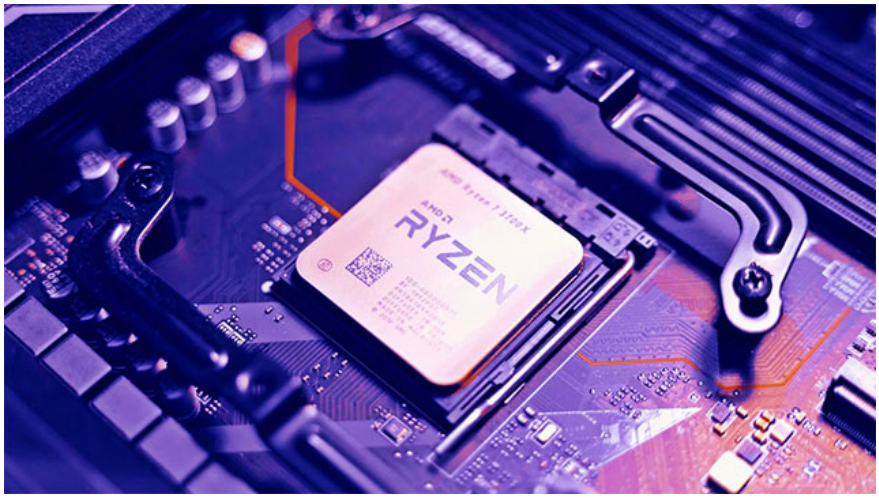
There is a serious security vulnerability that has existed for 18 years in AMD processors, but it is not too worrying

Security researchers at IOActive have discovered a serious vulnerability that exists in nearly two dozen AMD-branded CPU models.

An attacker could exploit this vulnerability to infect the CPU with malware and penetrate deep into the operating system. However, the good news is that this vulnerability is not easy to exploit, and AMD processor owners do not need to worry too much at the present time.

IOActive security experts call this vulnerability 'Sinkclose'. It has existed in PCs, data centers, and embedded AMD processors (chips used in cars or industrial equipment) for as long as 2006. To keep AMD chips backward compatible, manufacturers chip export added a feature that can modify privileged CPU configuration. That's the vulnerability that security researchers have found and exploited.

By abusing Sinkclose, malicious actors can modify processor configurations that are highly protected and only accessible through System Management Mode (SMM). System management operates at a higher privilege level than the operating system. And so, any changes made in this mode are 'invisible' and inaccessible to the operating system.



Threat actors could theoretically use this elevated access to install malware that runs at startup, known as before the operating system. Therefore, common processing procedures such as reinstalling the operating system, clearing memory or using anti-virus software are completely ineffective in eliminating this vulnerability. Instead, you will have to physically link it to the processor using a special programming device to detect and remove malware.

Fortunately, it is very difficult to execute an attack targeting this vulnerability. To start, an attacker will need kernel-level access - the kernel - which is the core that has complete control over the entire operating system. Modern operating systems have protections against unauthorized kernel access, so an attacker would have to bypass multiple layers of perimeter security to do so. Therefore, although the mining process is in fact present, the threat that Sinkclose poses is minimal to the average user.

In response to IOActive, AMD published a list of vulnerable processors along with some mitigation tips. The company is also implementing security patches for the affected processors.