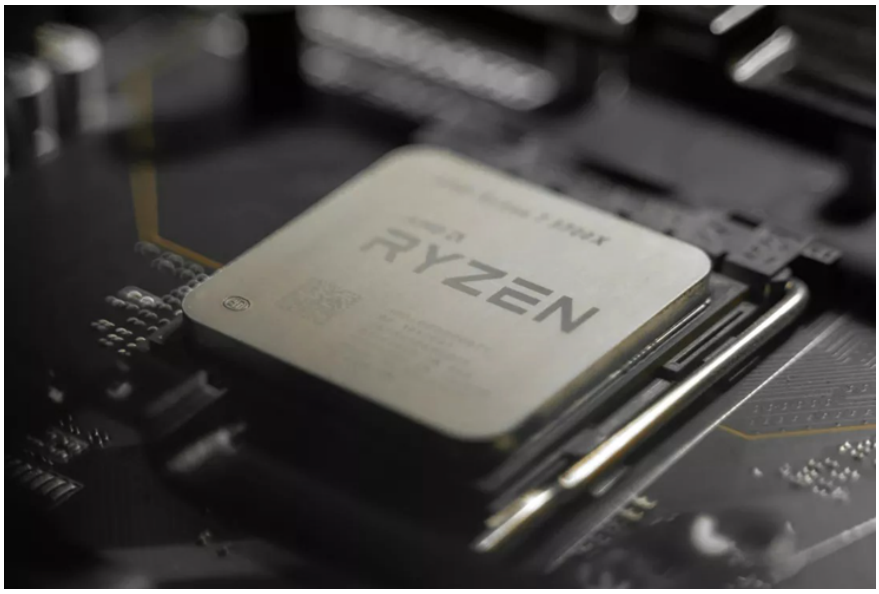
Serious security flaw discovered in AMD Zen chips

Google discovers 'death' vulnerability on all AMD Zen chips!

A serious security vulnerability has just been discovered by Google researchers, threatening millions of AMD Zen processors (CPUs) worldwide. This vulnerability can allow hackers to take complete control of the system, causing unpredictable consequences.

The "EntrySign" vulnerability affects all AMD Zen processors from Zen 1 to Zen 4 generations. By exploiting a flaw in AMD's microcode authentication process, an attacker can install custom microcode, changing the CPU's behavior at a fundamental level.



AMD Zen CPUs have dangerous vulnerabilities.

With control of the microcode, hackers can perform many sophisticated attacks, such as modifying the RDRAND instruction to generate fake random numbers, or even installing undetectable malware.

To aid in researching and fixing the vulnerability, Google has released zentool, an open-source 'cracking' toolkit that allows researchers to create, sign, and deploy custom microcode patches on vulnerable CPUs.

AMD responded quickly by releasing microcode updates that replaced the compromised authentication process with a custom secure hash function. Users are advised to update their CPU microcode to the latest version as soon as possible to protect their systems from potential attacks.

The EntrySign vulnerability is a reminder of the importance of ensuring hardware security, especially in the face of increasingly sophisticated cyberattacks.