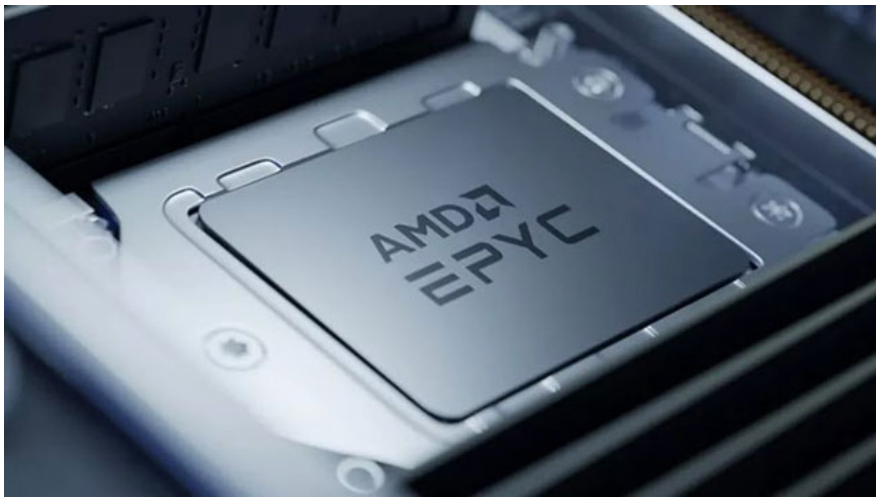
A dangerous vulnerability that has existed for 18 years threatens millions of AMD Ryzen and EPYC CPUs

Millions of computers running AMD Ryzen and EPYC CPUs worldwide are exposed to a dangerous vulnerability that allows attackers to run malicious code on the CPU when they are in System Management Mode, a sensitive mode that contains important firmware files.

The new vulnerability is called 'Sinkclose'. Hackers need to have deep access to computers or servers that operate on AMD processing systems to exploit this vulnerability. They can use bootkit malware - a type of malicious code that is difficult to detect and difficult to patch, to exploit vulnerabilities, thereby penetrating and controlling the system. Hackers will then install malware that is difficult to detect and can even persist even after reinstalling the operating system.



Although only recently reported, Sinkclose appears to have existed in many of AMD's CPU product lines, from desktops, workstations, servers to embedded devices and graphics solutions, for 18 years. pass without being detected.

AMD was notified about this vulnerability 10 months ago. The company has confirmed the existence of the Sinkclose vulnerability and has released patches for EPYC and Ryzen CPUs. The company also provides software and firmware patches to minimize the impact of the vulnerability.

To patch the vulnerability to ensure the safety of your system, AMD recommends that users update the latest BIOS.

many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.