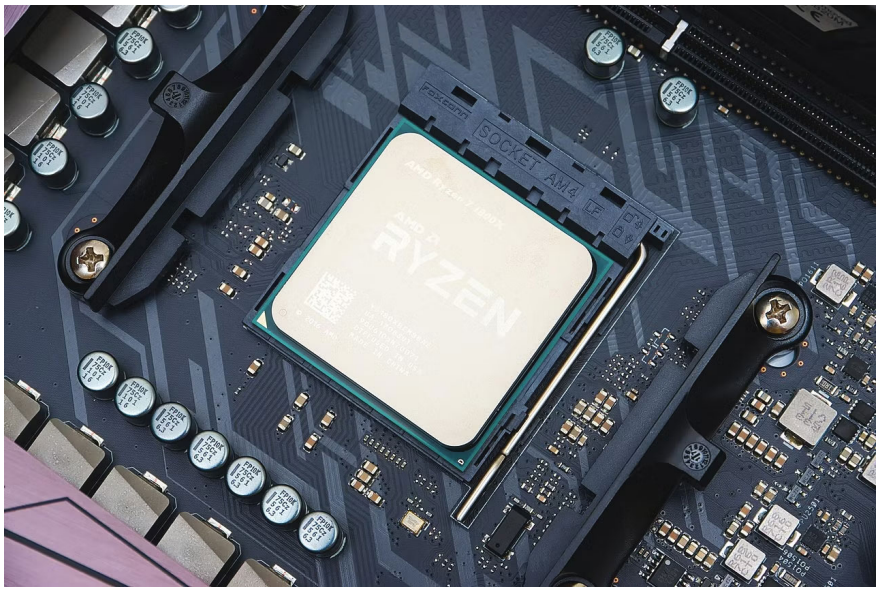
If you have an AMD CPU, install this important security update!

A nearly two-decade-old security flaw found in AMD silicon could leave millions of computers around the world vulnerable to nearly undetectable malware, but AMD is releasing patches to address the issue.

If you have an AMD CPU, you'll want to install the latest security updates for your CPU. A nearly two-decade-old security hole found in AMD silicon could expose millions of computers worldwide to nearly undetectable malware, but AMD is releasing patches to address the issue.

What is AMD CPU Sinkhole Security Vulnerability?

First disclosed by security researchers Enrique Nissim and Krzysztof Okupski at Def Con 2024, the AMD Sinkhole vulnerability could allow attackers to modify System Management Mode (SMM) settings, bypassing any existing protections.



If exploited, the installed malware would go undetected, as no antivirus or anti-malware program can detect malicious code running deep inside the CPU. SMM is one of the deepest operating modes of the CPU, used by the BIOS/UEFI to control power and hardware. Since the CPU is the core of the computer, it can allow access to other important components and information.

However, exploiting this vulnerability is not a simple process. It requires kernel-level access to the machine, which first requires another attack, in what is known as 'Ring 0 privileges'. Once set up on the device, the

attacker can attempt to enable 'Ring -2 privileges', gaining almost complete control of the device. It is the Ring -2 level of privileges that allows access to SMM settings, which are usually completely isolated from the operating system because of their importance.

Install AMD BIOS security patch

AMD's SMM Lock Bypass security notice details the affected CPUs:

`https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7014.html`

1. EPYC 1st, 2nd, 3rd and 4th Generation
2. EPYC Embedded 3000, 7002, 7003 and 9003, R1000, R2000, 5000 and 7000
3. Ryzen Embedded V1000, V2000 and V3000 Ryzen 3000, 5000, 4000, 7000 and 8000 series
4. Ryzen 3000 Mobile, 5000 Mobile, 4000 Mobile and 7000 series
5. Ryzen Threadripper 3000 and 7000 series
6. AMD Threadripper PRO (Castle Peak WS SP3, Chagall WS)
7. AMD Athlon 3000 series Mobile (Dali, Pollock)
8. AMD Instinct MI300A

This is a pretty long list, covering almost every AMD CPU from the past decade. Since the vulnerability wasn't discovered for nearly 20 years, it also covers a huge range of AMD CPUs, from consumer PCs to servers and more. You'll also note that AMD's newest processors, like the new 9000-Series CPUs, aren't on the list. While it's not confirmed, it's possible they were patched before release.

AMD has released BIOS/UEFI firmware patches to manufacturers for most modern CPUs – but told Tom's Hardware that some "older products are outside the scope of our software support." Still, AMD doesn't expect any performance issues on affected machines, which is a positive.

This means that AMD Ryzen 1000, 2000, and 3000 Series CPUs will not receive the Sinkclose patch. Whether that means you want to upgrade or move away from AMD is entirely up to you. Since this vulnerability can be extremely difficult to exploit, you don't need to upgrade right away. But it might be something to consider when upgrading your next PC.