

ZenBleed

Report Writing

ST5068CEM Platforms and operating Systems

Nisha Pandey

Student ID: 220321

Coventry ID: 13709947

Submitted to: Santosh Bhandari

Table of Contents

[History of CPU vulnerabilities 3](#_Toc152789468)

[Introduction of zenbleed 3](#_Toc152789469)

[How it works: 4](#_Toc152789470)

[Impact of the Zen Bleed 4](#_Toc152789471)

[Mitigation Strategies: 4](#_Toc152789472)

[Conclusion: 5](#_Toc152789473)

Zenbleed

# History of CPU vulnerabilities

CPU vulnerabilities are defects in a computer processor’s implementation or design that an attacker could use to obtain unauthorized access to the system or its data. Numerous things, including as side-channel attacks, hardware flaws, and software faults, might result in these vulnerabilities.

# Introduction of zenbleed

In recent years, CPU weakness have circulated regularly in and out of the news, and when they are revealed, they frequently carry a quite serious warning. It was that, in the circumstances of Zenbleed any computer program could access the stored data of any other program that was operating under the correct condition.

This vulnerability was discovered in 2019 and affects AMD's Zen processors. Google infosec expert Tavis Ormandy found the silicon level flaw that is known as the Zenbleed exploit. It affects Ryzen and Epyc Zen 2 CPUs, which are part of the AMD Zen2 CPU family, can be used to steal passwords, encryption keys, and other sensitive data.

Zenbleed is the term for a technique used by contemporary processors to increase performance by carrying out operations before they are required. It makes use of a feature found in modern x86 processors called vector registers that is used by operating systems and programs to decode strings and carry out mathematical calculations.

*It enables the attacker to inspect data as it is processed by applications and the operating system, which can include private information like passwords* (Adam,2023)*.*

# How it works:

Through the use of Zenbleed, which takes advantage of a weakness in AMD Zen processors’ handling of XMM register combining optimization, attackers can fool the processor into combining data from several processes into a single register. The attacker can then access this combined data by using a side-channel attack like Spectre.

1. XMM Register combine optimization: The attacker sets off a series of instructions that lead the processor to combine information from two distinct processes into one XMM register.
2. Register Rename: The combined register is given a new name by the processor.
3. Data Access: To obtain knowledge about the other process, the attacker reads data from the area of the register that hasn’t been cleared (Root, 2023).

# Impact of the Zen Bleed

The Zenbleed exploit significantly impacts the security of systems running AMD’s Zen 2 processors, including popular CPUs like the Ryzen 5 3600 and the entire Zen 2 product stack. The exploit allows attackers to steal data from any software on an impacted system. It’s also speculated that the Zenbleed exploit could slow down the performance of Zen 2 CPUs.

*One of the major concerns about Zenbleed is its ability to execute remotely without requiring physical access to a user’s computer.*

# Mitigation Strategies:

* Software Updates: AMD fixed the vulnerability with microcode updates. To take advantage of these mitigations, most update BIOS and oprating system to the most recent versions.
* Operating System Patches: To further reduce the attack surface, operating systems such as Linux executed kernel-level mitigations to limit access to L3 cache data.
* Hardware Mitigations: Some AMD processors from the latest generation have built-in hardware mitigations that reduce their vulnerability to Zenbleed (katz,2023).

# Conclusion:

A vulnerability known as Zenbleed, which affects AMD Zen processors, may allow malicious actors to access private data stored in the L3 cache. The possible effect on privacy and security of data cannot be disregarded, even though exploiting Zenbleed requires particular circumstances and expertise.

Reference:

Katz, E. (2023, November 6). *What is the 'Zenbleed' exploit and 7 ways to prevent it now*. Spectral. <https://spectralops.io/blog/what-is-the-zenbleed-exploit-and-7-ways-to-prevent-it-now/>

Root, E. (2023, August 18). *Zenbleed: Hardware vulnerability in AMD CPUs*. Kaspersky Cyber Security Solutions for Home and Business | Kaspersky.

<https://www.kaspersky.com/blog/zenbleed-vulnerability/48836/>

*Everything you need to know about CPU vulnerabilities like Zenbleed, downfall, inception, and more*. (2023, August 26). XDA Developers.

<https://www.xda-developers.com/cpu-vulnerabilities/>