THREAT ADVISORY

November 21, 2023

Reptar: A Newly Identified Intel CPU Vulnerability Affects Multi-Tenant Virtualized Environments

SUMMARY

Intel issued patches for a high-severity vulnerability named Reptar, which affects Intel desktop, mobile, and server CPUs.

RISK SCORING

CVE-2023-23583 8.8

VULNERABILITY DETAILS

The vulnerability may allow "escalation of privilege and/or information disclosure and/or denial of service via local access". Google (Google Cloud) provided results of their testings of this vulnerability, showing successful exploitation could allow bypassing the CPU's security boundaries, which was caused by how redundant prefixes are interpreted by the processor.

The impact of this vulnerability is even greater when exploited in a multi-tenant virtualized environment, where a guest machine is attacked and has the capacity to crash the host machine (cascading DoS). Additionally, the vulnerability poses the extended risk of information disclosure or privilege escalation.

There is no evidence of any active attacks using this vulnerability.

MITIGATIONS

Intel published updated microcode for all affected processors.

The complete list of Intel CPUs impacted by CVE-2023-23583 is available at:

Affected Processors: Transient Execution Attacks & Related Security... (intel.com)

REFERENCES

- https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/processors-affected-consolidated-product-cpu-model.html
- https://thehackernews.com/2023/11/reptar-new-intel-cpu-vulnerability.html