Multiple Vulnerabilities in Intel CPU

Severity Level: High

Components Affected

- Intel CPUs (desktop, mobile, and server CPUs)

Overview

A vulnerability have been identified in the Intel CPUs, which allow escalation of privilege, information disclosure, denial of service, bypass of the CPU's security boundaries via local access.

Description

The vulnerability which has been identified and tracked under CVE-2023-23583. The impact of this vulnerability is demonstrated when exploited by an attacker in a multi-tenant virtualized environment, as the exploit on a guest machine causes the host machine to crash resulting in a Denial of Service to other guest machines running on the same host. Additionally, the vulnerability could potentially lead to information disclosure or privilege escalation.

Impact

- Denial of Service
- Elevation of Privilege
- Security Restriction Bypass
- information disclosure

Solution/ Workarounds

Apply fixes issued by the vendor:

- https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/advisory-guidance.html

Reference

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

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.