Severity

Medium

Analysis Summary

CVE-2022-0005

Intel Software Guard Extensions (SGX) Platform could allow a local authenticated attacker to obtain sensitive information, caused by an unspecified flaw. By physically probing the JTAG interface, an attacker could exploit this vulnerability to obtain sensitive information.

Impact

- Information Disclosure

Indicators Of Compromise

CVE

- CVE-2022-0005

Affected Vendors

- Intel

Affected Products

- Intel 8th Gen Intel Core Processor
- Intel 8th Generation Core Processor Family
- Intel 7th Generation Core Processor Family
- Intel 6th Generation Core Processor Family

Remediation

Refer to INTEl Security Advisory for patch, upgrade or suggested workaround information. INTEl Security Advisory