# CVE Detail – CVE-2020-9285

Some versions of Sonos One (1st and 2nd generation) allow partial or full memory access via attacker controlled hardware that can be attached to the Mini-PCI Express slot on the motherboard that hosts the WiFi card on the device.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.10767

## CVSS Scoring

CVSS v3.1 Score: 6.8

Severity: MEDIUM

## Mapped CWE(s)

* CWE-1191: On-Chip Debug and Test Interface With Improper Access Control

## CAPEC(s)

* CAPEC-1: Accessing Functionality Not Properly Constrained by ACLs
* CAPEC-180: Exploiting Incorrectly Configured Access Control Security Levels

## ATT&CK Techniques

* T1574.010: Services File Permissions Weakness

## Used By (Actors/Tools)

* BlackEnergy (malware)

## Affected Products

* cpe:2.3:o:sonos:one\_firmware:-:\*:\*:\*:\*:\*:\*:\*