# CVE Detail – CVE-2019-18673

On SHIFT BitBox02 devices, a side channel for the row-based OLED display was found. The power consumption of each row-based display cycle depends on the number of illuminated pixels, allowing a partial recovery of display contents. For example, a hardware implant in the USB cable might be able to leverage this behavior to recover confidential secrets such as the PIN and BIP39 mnemonic. Note: BIP39 secrets are not displayed by default on this device. The side channel is relevant only if the attacker has enough control over the device's USB connection to make power-consumption measurements at a time when secret data is displayed. The side channel is not relevant in other circumstances, such as a stolen device that is not currently displaying secret data.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.34542

## CVSS Scoring

CVSS v3.1 Score: 4.6

Severity: MEDIUM

## Mapped CWE(s)

* CWE-203: Observable Discrepancy

## CAPEC(s)

* CAPEC-189: Black Box Reverse Engineering

## Affected Products

* cpe:2.3:h:shiftcrypto:bitbox02:-:\*:\*:\*:\*:\*:\*:\*