# CVE Detail – CVE-2021-38759

Raspberry Pi OS through 5.10 has the raspberry default password for the pi account. If not changed, attackers can gain administrator privileges.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.97434

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-1188: Initialization of a Resource with an Insecure Default

## CAPEC(s)

* CAPEC-665: Exploitation of Thunderbolt Protection Flaws

## ATT&CK Techniques

* T1542.002: Component Firmware
* T1556: Modify Authentication Process
* T1211: Exploitation for Defense Evasion

## Used By (Actors/Tools)

* Cyclops Blink (malware)
* Kessel (malware)
* Ebury (malware)
* SILENTTRINITY (tool)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Equation (intrusion-set)
* APT28 (intrusion-set)
* FIN13 (intrusion-set)

## Affected Products

* cpe:2.3:o:raspberrypi:raspberry\_pi\_os\_lite:\*:\*:\*:\*:\*:\*:\*:\*