# CVE Detail – CVE-2020-15483

An issue was discovered on Nescomed Multipara Monitor M1000 devices. The physical UART debug port provides a shell, without requiring a password, with complete access.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.1252

## CVSS Scoring

CVSS v3.1 Score: 6.8

Severity: MEDIUM

## Mapped CWE(s)

* CWE-306: Missing Authentication for Critical Function

## CAPEC(s)

* CAPEC-12: Choosing Message Identifier
* CAPEC-166: Force the System to Reset Values
* CAPEC-216: Communication Channel Manipulation
* CAPEC-36: Using Unpublished Interfaces or Functionality
* CAPEC-62: Cross Site Request Forgery

## Affected Products

* cpe:2.3:o:niscomed:m1000\_multipara\_patient\_monitor\_firmware:-:\*:\*:\*:\*:\*:\*:\*