

Technical Advisory

Through sharp, technical and insightful analysis, the Payatu Team is constantly on the lookout for vulnerabilities and threats. This section exhibits a few of our findings.

Unauthenticated UART port in niscomed patient monitoring device

Vulnerability

Unauthenticated UART port in niscomed patient monitoring

Vulnerability Description

An issue was discovered on Nescomed Multipara Monitor M1000 devices. The physical UART debug port provides a shell, without requiring a password, with complete root access. This leads to compromised medical data and integrity of the device.

CVE-ID

CVE-2020-15483

Vendor

Nescomed

Product

M1000 Multipara Patient monitor

Disclosure Timeline

22 June 2020 reported to the vendor

22 July 2020 No response from the vendor and Public disclosure.

Credit

Arun Magesh



Research Powered Cybersecurity
Services and Training. Eliminate security
threats through our innovative and
extensive security assessments.

Subscribe to our newsletter

Enter your email address.



Services



Products



Conference



Resources



About



All rights reserved © 2022 Payatu



Research Powered Cybersecurity
Services and Training. Eliminate security
threats through our innovative and
extensive security assessments.

Subscribe to our newsletter

Enter your email address.



Services

IoT Security Testing
Red Team Assessment
Product Security
AI/ML Security Audit
Web Security Testing
Mobile Security Testing
DevSecOps Consulting
Code Review
Cloud Security
Critical Infrastructure

Products

EXPLIoT
CloudFuzz

Conference

Nullcon
Hardwear.io

Resources

Blog
E-Book
Advisory
Media
Case Studies
MasterClass Series
Securecode.wiki

About

About Us
Career
News
Contact Us
Payatu Bandits
Hardware-Lab
Disclosure Policy

