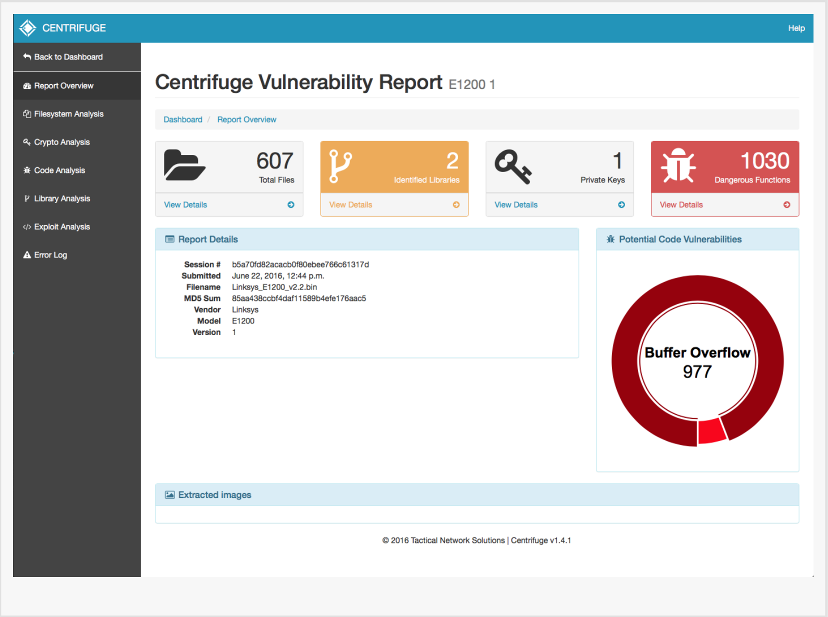
EIN PRESSWIRE

Tactical Network Solutions Issues Sample IoT Security Report with Firmware Backdoors Often Found in Medical Devices

Medical device manufacturers must raise their security awareness around their vulnerable connected medical devices.

COLUMBIA, MD, USA, June 1, 2017 /EINPresswire.com/ -- The extremely high number of connected medical devices rapidly coming to market has consumers and manufacturers excited. The new IoT devices often include medical advancements, more effective data collection and greater ease of use. But, when the devices are not built securely, they also bring unnecessary exposure, vulnerabilities and danger.



Centrifuge Vulnerability Report E1200 1

Report Details

Session #	b5a70fd82acacb0f80ebee766c61317d
Submitted	June 22, 2016, 12:44 p.m.
Filename	Linksys_E1200_v2.2.bin
MD5 Sum	85aa438ccbf4daf11589b4efe176aac5
Vendor	Linksys
Model	E1200
Version	1

© 2016 Tactical Network Solutions | Centrifuge v1.4.1

To support medical device manufacturers and others in the connected healthcare space, Tactical Network Solutions (TNS) has issued a sample report that uncovers security flaws in a connected device. The 17-page report illustrates firmware vulnerabilities including hidden backdoor accounts, private security keys and 3rd party library vulnerabilities.

The report was produced with data gathered from Centrifuge, their custom-built IoT Security Platform, which automatically reverse engineers compiled firmware images to uncover security holes. Centrifuge extracts the complete root filesystems within the firmware images, deconstructs each file down to the bytecode level and provides reporting on vulnerable functions calls. This process gives medical device manufacturers a bird's eye view into potentially dangerous and exploitable security issues on their devices.

As the IoT medical device market rapidly expands, companies will continue to automate as much of the firmware evaluation process as possible. TNS is working to bring tools and solutions to healthcare companies and others in this space who seek accurate and timely security evaluations of connected medical devices.

About Tactical Network Solutions: Fortune 500 companies and governments around the world come to Tactical Network Solutions for our reverse engineering training programs, firmware evaluations and cyber risk mitigation strategies. TNS discovers hidden attack vectors in IoT and other connected devices using the Centrifuge IoT Security Platform to rapidly conduct firmware evaluations and mitigate cyber risks.

Gina Palladino

Tactical Network Solutions LLC
443-276-6990
email us here

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.