NETRISE

Next-Gen XIoT Security Platform

Is Your Firmware a Soft Target?

Firmware is the trusted foundation for every hardware device. Whether that device is a security camera, Programmable Logic Controller (PLC), infotainment system in a car or a pacemaker in a person's body, firmware is what controls them.

Traditional XIoT security products only focus on the operating systems and configuration settings of devices while neglecting the actual code that is running – XIoT firmware has been treated like a black box as end-users have had minimal control over it

The end result is that many organizations – even ones with rigorous vulnerability management programs – effectively ignore the risks of XIoT firmware.

This lack of insight and analysis leaves a gaping hole in most organizations' security programs.

As device proliferation grows at an exponential rate due to the rapid adoption of 5G and the sudden transition to remote or hybrid work, it is critical that organizations have full insight into the risks posed by insecure firmware.

Introducing The NetRise Platform

NetRise is the first platform to provide comprehensive insight into shared vulnerabilities across all XIoT firmware images in an organization. These risks and associated artifacts are presented in a clear and concise manner allowing consultants, operators, and SOC analysts alike to take appropriate action and address the firmware-based threats to an organization.

NetRise is a cloud- based SaaS platform that receives firmware images via upload or API. The firmware images are then dissected, presenting all of the key data, artifacts, and risk in an easy-to-consume interface. The end result is that NetRise reduces the time and cost of firmware security programs allowing organizations to quickly find and remediate previously undetected issues.

netrise.io | sales@netrise.io

Copyright © 2023 NetRise, Inc.