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

NETRISE

Use Cases

How many of my devices possess a particular vulnerability?

How prevalent is a particular file within the devices in my environment?

Are any of my devices using default or easily guessed credentials?

Are there any backdoors present in my devices?

Are my devices compliant with industry standard frameworks?

How does my device risk compare across vendors?

Features & Benefits

Complete Visibility

Evaluating the risk of firmware is much more than simply understanding how many vulnerabilities are present. NetRise uncovers repeat vulnerabilities found across all products in an organization, provides clear prioritization of risks and reduces the time it takes for human responders to apply context to complex problems. The NetRise Platform goes beyond merely utilizing the Common Vulnerabilities and Exposures (CVE) catalog when assessing risk, enabling remediation efforts with the most accurate firmware risk scoring, including:

- The Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) Catalog
- Known usage of an exploit by botnets, ransomware groups, or other threat actors
- Marketing nomenclature raising awareness, such as Ripple20, Log4j, and others
- Availability and weaponization of an exploit via toolkits and other easy to use methods
- Misconfigurations, leaked credentials, and more

Continuous Monitoring

Firmware is often developed and once released does not undergo another assessment for the lifetime of the product. Traditional cybersecurity providers only look at a “slice-in-time” of a firmware instance during a vulnerability assessment. With more and more attacks are targeting firmware directly leading to nearly undetectable persistence mechanisms. NetRise solves these problems by continuously monitoring and analyzing artifacts within firmware to identify and prioritize:

- Vulnerabilities – known and unknown
- Compliance Adherence – publicly available or build your own
- SBOM – SPDX, CycloneDX
- Overall Risk – configurable weightings

Ready for a Demo?

netrise.io | sales@netrise.io