NETRISE

A GUIDE TO

XIoT Firmware Security

The non-traditional operating systems XIoT devices run on have quickly made them a prime target of adversaries. Firmware security is essential to securing devices and the networks they operate on.

Overview

Why Does XIoT Security Matter?

When Extended Internet of Things (XIoT) devices sit on the public internet, they are often too easy a target for hackers. XIoT comprises the Internet of Things (IoT), Operational Technology (OT), medical devices, and other connected devices. While it may not be the goal of a cyber incursion to hack your thermostat, for example, access can enable deeper reach into the networks and systems critical to operations. This is where firmware security for XIoT devices comes into play.

Why is XIoT Firmware Security Important?

Extended Internet of Things (XIoT) devices are commonly seen as black boxes. The firmware XIoT operates on is largely unknown to most asset owners and sometimes even to the device manufacturer. As devices move down the factory line, hardware and software are added and packaged up in preparation for the market. Are device manufacturers aware of every component that goes into their products? Who is inspecting the final product for vulnerabilities and what security assurances can a manufacturer give their customers?

The problem is compounded by the fact that there is little control exerted over the security features of devices, and it's never top of mind. While you can easily add antivirus protection and configure controls for a laptop, it's nearly impossible for XIoT devices.

Other firmware security challenges manufacturers face:

- Complexity related to having multiple suppliers and sources in firmware supply chains
- Lack of tools to inspect the final product firmware
- End user inability to customize device configurations and improve security posture
- Shipping with default settings the end user is expected to change (but doesn't)

Why Securing Firmware is Important

For Device Manufacturers

- Ensure the devices they create are secure and free from unaddressed risk
- Avoid liability if a device they created causes a security issue in a customer's environment
- Meet compliance with the latest security regulations related to firmware and supply chains

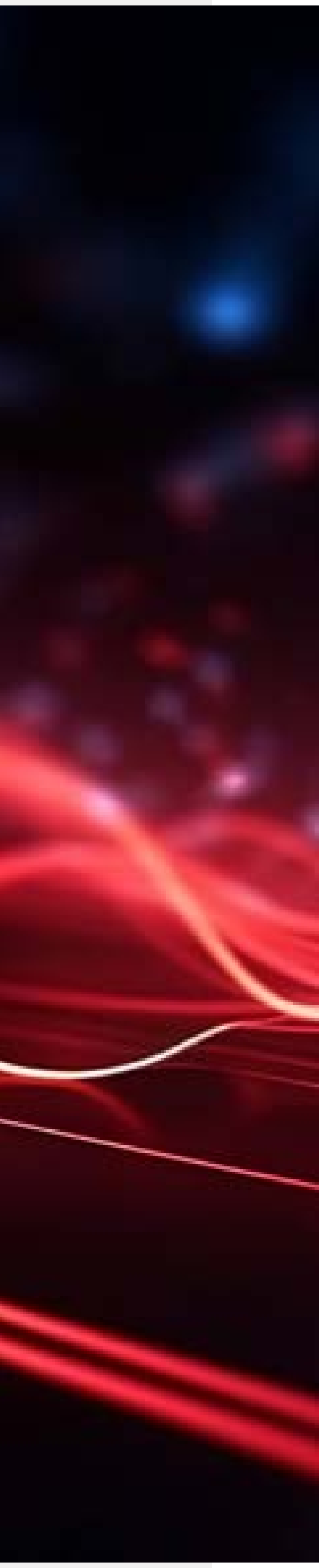
For Asset Owners

- Identify and assess the risks associated with adding new devices or patching existing ones
- Reduce the risk of device firmware, which makes up the largest enterprise attack surface
- Understand the critical role firmware has in responding to component vulnerabilities

Executive Order 14028

In May 2021, the Biden Administration announced Executive Order 14028 in an effort to improve the nation's cybersecurity. The mandate requires device manufacturers to pay attention to their upstream and downstream supply chains. They're required to provide transparency into where all their device components came from, along with any known vulnerabilities. To do this, they're expected to generate a software bill of materials (SBOM) for each device.

The coordination of enforcing Executive Order 14028 is still in its beginning phases, but we expect enforcement will be in the form of government audits, with noncompliance resulting in fines. This executive order represents a first step toward broader government regulation requiring effective SBOM management from manufacturers and indicates the potential for loss of revenue and business growth opportunities for those who are slow to adapt.



Risks Associated With Known Firmware Vulnerabilities

XIoT devices are frequently brought to market with already known vulnerabilities, a reality most manufacturers have little to no visibility into. How do these hidden risks affect asset owners?

Business Disruption

When a device is exploited or compromised, it exposes your organization to ransomware, loss of intellectual property, loss of business, network downtime, and other potential impacts.

Learn About Holistic Visibility

Loss of Trust

When organizations are the victim of a breach, public trust drops, especially when personal identifiable information (PII) is exposed, industry regulations like HIPAA are violated, or bodily injury and loss of life occur as a result.

Learn About Compliance Adherence

Software Risks and Understanding Your Software Supply Chain Security

NetRise CEO Thomas Pace and Fortress Information Security's Bryan Cowan discuss software and device risk, supply chain security, and the lifecycle of different use cases in this webinar.

Watch the Webinar ▶

How Hackers Exploit Firmware Vulnerabilities

Firmware vulnerabilities can be exploited just like any other device vulnerability. Without adequate remediation of device risks, hackers can go undetected for longer periods of time. While firmware or software components within XIoT devices such as printers may not be a hacker's ultimate goal, unaddressed vulnerabilities within firmware and software can provide easy access to higher-value targets within an organization.

Examples of how hackers exploit firmware vulnerabilities

- A backdoor is created either intentionally (by a hacker) or unintentionally (by the device manufacturer or end user)
- A device comes with hard-coded passwords and no option to change them
- A device comes with a standard password, but the asset owner doesn't change it

What Happens During an Attack on an XIoT Device

Typically, an attacker finds an unaddressed vulnerability within the firmware or software supply chain. Once compromised, the device can be leveraged as the attacker sees fit. Users may notice the device exhibiting abnormal behavior or be unable to login to or control the device, or there may be little to no signs of incursion.

Attacks can also occur when an asset owner receives a disingenuous firmware or software update and loads it into a device thinking it is a normal update, at which point the device is compromised.

Examples of how this happens:

Mirror Sites

Instead of typing the correct, official web address, a user types in the wrong URL, taking them to a mirror site of the site they are familiar with when downloading updates. If the user goes through the process of logging in and downloading an update from the mirror site, it could compromise their device.

Phishing Emails

An email may look like it comes from a big OEM, but it's actually a phishing attempt. If the user clicks through and downloads the update, they're compromised.

Vendor Update Process Compromise

In rare and unfortunate cases, compromised vendors have unknowingly delivered a hacker's payload via apparently official update processes. In these unusual circumstances, it is especially critical to have the capability to assess patches before deployment.

Attackers also use vulnerabilities as distractions to get to their end goal. They may make your printer malfunction, so your security team's focus is there while they work their way deeper into your network.

Steps to Take When Your Device or Supply Chain Has Been Compromised

To protect your network and its users, follow these steps.

01 **Take the device offline**
Immediately take the device off your network.

02 **Analyze the firmware**
Conduct firmware analysis to find vulnerabilities.

03 **Update firmware**
Work with the OEM to get a validated copy of firmware.

04 **Determine spread**
Was the attacker able to move laterally beyond this device? Question everything the device can interface with.

05 **Conduct tests**
Test the restored device in a safe environment before returning it back to service.

06 **Return to environment**
Return the tested device back to your network.

When to Conduct A Firmware Update

Firmware updates typically come at the recommendation of the device OEM. If the update is security-related, install it as soon as possible. Again, be wary of phishing and make sure firmware is genuine by verifying it with the OEM. NetRise customers can take the additional step of analyzing the new firmware version for vulnerabilities before deployment, enabling safer procurement and patching.

- Implement buffer and stack overflow protection
- Perform firmware updates and ensure cryptographic signatures
- Capture security exceptions
- Validate all user input
- Perform regular security code reviews
- Optimize how data is collected, used, and stored

Firmware Security with NetRise

The NetRise platform helps device manufacturers and asset owners gain visibility into devices typically treated as black boxes by security and IT teams. The platform highlights and prioritizes vulnerabilities, misconfigurations, and other risks associated with device firmware. However, it's up to security teams to remediate or address the risks.

To learn more about these devices, NetRise conducts Binary Composition Analysis (BCA) and generates a software bill of materials (SBOM) to identify every component in the device.

NetRise Trace utilizes AI-powered intent interpretation to allow users to look for assets based on the motives behind code and configurations rather than relying on traditional signature-based methods. Trace helps organizations quickly trace impacted assets with a single query, creating a comprehensive graph of affected software supply chain components and their associated vulnerabilities. This eliminates the need for repetitive scans and accelerates the response to threats across devices, firmware, and software packages.

Benefits of analyzing XIoT devices with NetRise:

- Generate, ingest, enrich, and inventory comprehensive SBOMs
- Access to vulnerability correlation, enrichment, and prioritization
- Enumeration of binaries and protection mechanisms
- Insight into certificates, public keys, and private keys
- Identification of credentials and other secrets
- Misconfiguration risk identification
- Search capability to perform real-time searching across all devices in the event of a breach

Ready to See NetRise in Action?

Schedule a NetRise platform demo, and learn more about how NetRise can improve your IoT security posture today.

Contact Us

NETRISE

in f 𝕏 ▶

netrise.io | sales@netrise.io