It’s Time to Solve the Dangers Communication Service Providers Face Lurking in Their Firmware

A broken lock puts one satellite office at risk for thousands of dollars in damage, lost equipment, and potentially the need to reroute traffic to keep your network secure. However, if the broken lock is in your latest set-top box, router, modem, or even headend, it immediately becomes a network-wide problem with the potential to do millions of dollars in immediate damage as well as long-term reputational harm.

Firmware that is poorly coded or contains purposeful exploits is the flimsy lock we are talking about, and it remains one of the greatest threats to any service provider.

The average data breach will cost a company more than $3.86 million, according to IBM analysis. For the Communication Service Provider (CSP), however, data breaches can occur on both your network and the networks you build for your customers. If you are found at fault, then you may face costs for the damage to both networks, yours as well as theirs. And when the threat targets firmware, there is no single or short-term risk.

Industry has seen such dangers before, most recently with the Mirai botnet. In October 2016, the Mirai botnet took down roughly 14,500 web domains that used Dyn’s managed DNS service, and cost the company a projected $110 million in what would have been potential revenue. The following month, the botnet exploited more faulty devices and knocked 900,000 Deutsche Telekom routers offline for days, leading to roughly $1.96 million in costs, not to mention damaging a brand reputation.

When Paras Jha, an undergraduate at Rutgers, pled guilty to crimes related to the Mirai attacks, he confirmed that the code was already in the wild and likely being used as a basis for future botnets from others.

The firmware danger still exists. Product security teams must take note and address the danger, as well as the risks, for all the firmware exploits currently known and those soon to be discovered. Safety requires a commitment from a CSP to use the best analytical tools to obtain the highest level of security.

refirm labs

CASE STUDY

Addressing Partner Firmware Risks

Unfortunately for the industry, the quality of today's firmware is widely recognized as insufficient to handle evolving threats. Poor coding quality and outsourcing habits often result in attack vectors that compromise your devices.

Firmware remains one of the largest gaps in supply chain risk management. When vulnerabilities in firmware are missed and an unsafe device lands in the hands of customers, it's often too late to avoid costly mistakes.

CSPs must rethink their product security schemes to address known risks, potential zero-day exploits, and malicious internal or external actors. This requires going beyond penetration testing that looks at the security of the device from only one angle, and reaching into the firmware that powers your devices to safeguard customers and their data during real-world usage.

Vendors may initially create the risks CSPs face, but the provider is responsible for preventing all threats to their customers. You can protect your entire supply chain by working with vendors and ReFirm Labs to uncover firmware dangers.

Do you have a plan to address and mitigate the risks that vendor and partner firmware pose to your organization?

Types of Vulnerabilities in Embedded/IoT Devices

Vulnerability	Implications of the vulnerability
Unauthenticated access	Allows unfettered access, making it trivial for attackers to gain access and controls of the device.
Weak authentication	Simple password-based authentication or weak cryptographic algorithms than can be broken by brute force attacks.
Hidden back-doors	While potentially helpful for customer support, they are staple features that hackers quickly identify and exploit, often with severe consequences.
Password hashes stored in firmware	Hard-coded passwords that users are unable to change, and default passwords that users rarely change, result in devices that are trivial to exploit. Exploited by the Mirai malware to create a botnet of roughly 2.5 million IoT devices.
Encryption keys stored in firmware	Encryption keys are critical, but when stored in firmware, they can result in easily compromised devices.
Buffer overflows vulnerabilities	Use of insecure string handling functions such as strcpy, strcat, etc., instead of their more secure strncpy, strncat counterparts, may result in buffer overflows that can be exploited, creating denial of service and code injection attacks.
Use of open source solutions with known vulnerabilities	Automated hacking tools include exploits targeting known vulnerabilities in open source platforms and libraries. The latest versions will frequently include fixes, yet many devices are released un-patched.
Debug services in production systems	While critical during development and testing, they provide unfettered access and control over the device.

Recent Firmware Attacks

Mirai 2016 Botnet Attack

- Scanned for open Telnet ports and attempted to log in with 61 default username and password combinations, including some hardcoded options.
- October 2016: Famously took out access for much of the U.S. to popular sites including GitHub, Twitter, Reddit, Netflix, Airbnb, and others.
- November 2016: Crashed nearly 900,000 routers produced by Arcadyan due to failed TR-064 exploitation attempts by a variant of Mirai

Deploying Always-Available Firmware Protection

Comprehensive supply chain risk management is possible when you use the best tools available on the market. One solution to consider for protecting your firmware and IoT devices is the Centrifuge Platform™, from the creators of binwalk, the leading firmware extraction tool on the market.

The Centrifuge Platform™ is an enterprise-grade firmware analysis tool that can indicate poor firmware security and potential exploits in the devices your business relies on for continuous revenue.

"Centrifuge consolidates 30 of the work steps into one convenient dashboard," says a network security engineer at one of America's fastest growing TV, internet, and voice companies. He noted the company found hundreds of vulnerabilities within its vendor's cable modem headend termination systems.

It is crucial to generate detailed visibility into the underbelly of firmware on the products you offer, no matter how long they've been under development or in the field. Check every set-top box (STB) in minutes and keep your network and devices from becoming points of failure, data thefts, or unwilling participants in the next botnet attack.

Discover More with Your Data and Partners

The Centrifuge Platform™ offers CSPs the ability to work effectively with their vendors to uncover threats and provide a more reliable service. Our analysis offers a neutral platform for service providers to understand their devices— which is only set to grow as IoT offerings expand — and discuss threat resolution with vendors.

You'll receive an objective analysis of devices through rapid firmware testing to ensure that your network and customers are secure. The Centrifuge Platform™ supports new equipment as well as equipment that is already in the field. Develop your own pass/fail criteria to mitigate and manage the risks that a modern network faces each day. With our Centrifuge Guardian™ protection, you also get proactive notifications when new vulnerabilities are discovered after you've deployed the device on your network. It's protection for the long haul.

Now, it's time to test this with your existing network. ReFirm Labs is providing a full trial of The Centrifuge Platform™, generating complete reports for a number of your devices. Contact us today to learn how you can understand the threats your STBs, modems, routers, head ends, and many other devices face.

SCHEDULE YOUR FREE CONSULTATION

Centrifuge Features

Proactively detects and protects against potential zero-day exploits, public vulnerabilities, crypto keys, and potential backdoors

Guardian continuously monitors and alerts when new vulnerabilities are found in previously analyzed firmware

Subject matter experts (SMEs) available for ongoing support and analysis including exploit proof-of-concepts

No need for agents on your network or SDKs embedded in the device

Works for cloud and on-premise deployments

API integration supports third-party tools and workflows

No source code required

Delivers software bill of materials (SBOM) and other tool lists

Recent Customer Successes

altibox

A Norwegian ISP, servicing nearly a quarter of the country's TV and Internet market, used Centrifuge to test existing STBs and determined some models did not meet existing security requirements. As a result, they are changing their hardware profile to match firmware implementations that better safeguard their customers.

AT&T

A nationally recognized US telco has chosen the Centrifuge Platform™ to understand their firmware on legacy products better. Our reporting, combined with external penetration testing, is improving their company's ability to get all STBs up to the desired standard and protect against additional concerns such as encoded private keys.

Charter COMMUNICATIONS

A well-known telco and cable provider is using Centrifuge to analyze its CPE, including cable modems and L3 routers, to provide a single dashboard for firmware analysis. We identified roughly 500 vulnerabilities in a single piece of equipment.

Firmware Threats Centrifuge Has Identified

Backdoor accounts, including potential purposeful inclusion

Weak default passwords that were broken within a few hours

Multiple password hashes located in devices

Private signing crypto keys, including known and unknown items

Specific code flaws that can be crashed and turned into exploits

Open source libraries that have 10-year-old critical vulnerabilities still present