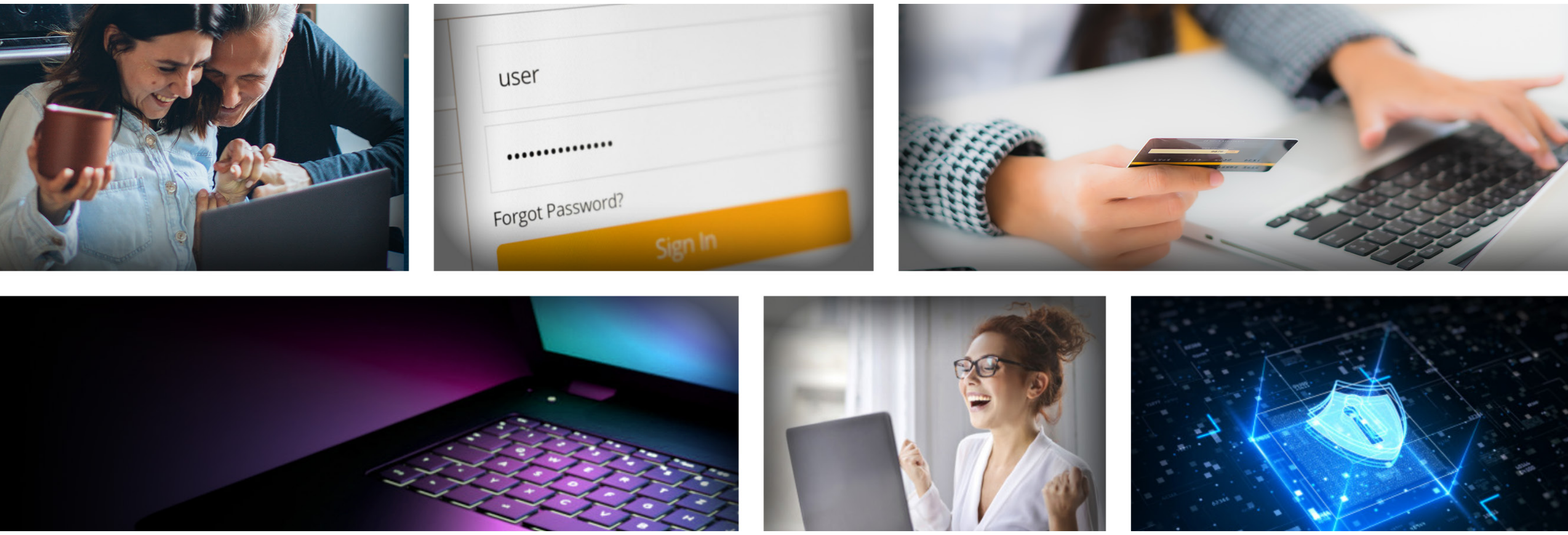


How to Deploy Secure CPE and Wi-Fi Routers

A guide for service providers

Your subscribers are using their broadband service, and their home network, far more than ever before. Unfortunately, hackers have identified subscriber home networks and Wi-Fi routers in particular as rich targets for malicious attacks. This creates some serious challenges for broadband service providers looking to protect their subscribers, network, and brand. Here we explore how hackers target Wi-Fi routers and how to keep security at the forefront of your CPE development and deployment.

The threat to your subscribers is real

Over the last several years, the number and kinds of attacks on your subscribers' home networks have increased exponentially. With more and more devices connected to the average user's network, there are plenty of potentially vulnerable targets to exploit.

What do hackers want from home networks?

They want to mine for sensitive data

With services offered through the cloud such as home automation, telehealth, and internet banking, subscribers entrust their privacy and security to their broadband service, transmitting sensitive data more freely and more often.

By compromising the home network, malicious agents can mine for sensitive information like credit information, login credentials, or other personal data. Attackers circumvent encrypted communications by intercepting and redirecting web traffic (e.g., through DNS spoofing or other methods) to pages that look legitimate but capture user data.

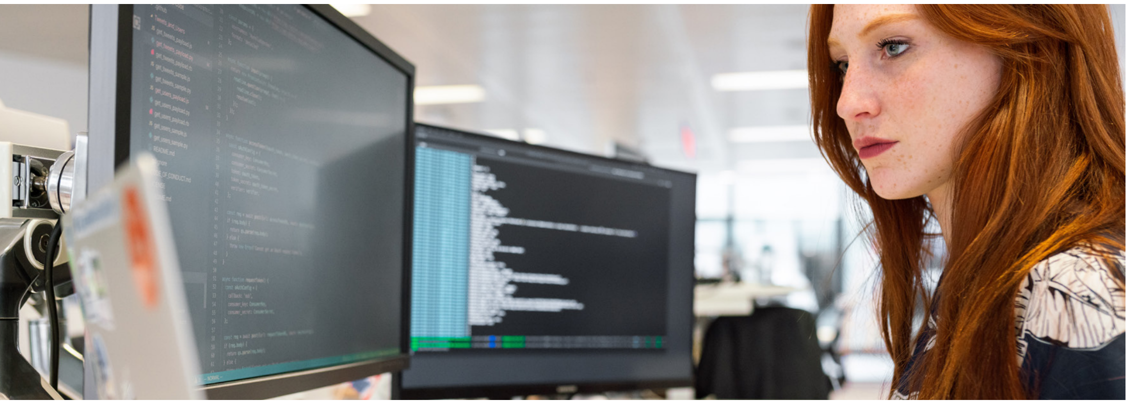
They want to exploit computing resources

Perhaps the most common goal of a malicious attacker is to exploit the computing resources of hijacked devices. As home Wi-Fi routers become more sophisticated, they also have more CPU and memory available. This makes them a particularly attractive target for attackers.

Worms and botnets often spread specifically to use other systems for Distributed Denial of Service (DDoS) attacks, or to use resources to continue to spread malware to more and more systems. Cryptocurrency mining is another use of hijacked computing resources. An end-user may not even know that their devices are compromised.

They may even jump to extortion

Hackers may even be bold enough to activate ransomware on a subscriber's computers, locking down files and holding their data hostage until demands are met, usually in the form of payment in cryptocurrency. When more people are working from home, this can be dangerous not only to your subscriber but also to their employer.



Recent attacks

THE MIRAI WORM

The goal of the Mirai Worm (2016) attack was to get these routers to execute arbitrary code and download the Mirai malware, making them robots for DDoS attacks. The attack exploited three distinct vulnerabilities: use of a deprecated protocol (TR-064), serving that protocol on an open port not intended for use, and code injection in the protocol messages.

VPNFILTER

The malware dubbed VPNfilter (2018) performed intelligence-collection on a compromised device, mining for user credentials and other sensitive data. It was downloaded to routers known to have public exploits or those that used default credentials that made compromise relatively straightforward.

GHOSTDNS

GhostDNS malware (2018) modified the DNS settings of compromised devices to send users to false websites to gather credentials, credit card information, and more. It systematically searched for routers that used weak or no password at all, accessed the routers' settings, and then changed the router's default DNS address to the one controlled by the attackers.

Why target the Wi-Fi router?

Hackers are targeting home Wi-Fi routers because they are valuable resources and are often very easy to exploit. Without active management, they can go long periods without being patched or upgraded. Retail devices see this issue more acutely. It is usually left to the end-user to keep their devices up-to-date, so known "zero-day" vulnerabilities (i.e., haven't been seen before) remain exploitable.

However, very few vulnerabilities in Wi-Fi routers are considered zero-day. More often, vulnerabilities arise from common mistakes made in designing CPE. Many of these mistakes exist because of legacy choices made at the Original Equipment Manufacturer (OEM) or System-on-a-Chip (SoC) level for ease of use or ease of development. Indeed, the vast majority of vulnerabilities that have made the headlines are oversights like easy-to-guess default passwords, a lack of (or poorly implemented) TLS on a device's interfaces, or unnecessary services running on devices by default.

Without proper testing and firm requirements from service providers, these vulnerabilities persist even today.

Service providers should take charge of CPE security

Whether your CPEs are provided to subscribers by you or through the retail market, you have both the responsibility and opportunity to ensure the Wi-Fi router's security. Insecure devices make insecure networks, and ultimately makes your company just as vulnerable as the subscribers under your purview.

Avoid the cost of security breaches

The CAPEX/OPEX cost of mitigating an attack, patching and distributing firmware, and handling the support load can quickly get out of hand. Catching vulnerabilities ahead of time and reducing them altogether saves money and boosts Average Revenue per User (ARPU).

Protect your entire network

Once an attacker gains a foothold in your subscriber's network, the potential risk to other subscribers and your broadband network increases significantly. The subscriber's network is a part of your network, and you should act with that in mind.

Stay compliant with regulations

Depending on your region, governments may have end-user privacy protections written into regulations that you must adhere to as a broadband service provider. Security breaches that compromise privacy may fall under your responsibility, opening your company to fines or other penalties.

Avoid brand damage

No company wants to see their name on the home page of Ars Technica, featured as the latest subject of a massive router security breach. Brand damage is harmful to your organization, demoralizes support and product teams, and ultimately hurts your bottom line.

Guidelines for securing your CPE

As a service provider, you have control over the deployment of CPE in your network. This control gives you the power to put security first in the design and development of those CPE. It is best to think of security as a process goal and understand how all your activities impact it.

There are four key points to stick to when ensuring secure devices:

☑ Understand your device ecosystem.

☑ Require best practices.

☑ Make regular testing part of your process.

☑ Work with your vendors.

Let's explore each of these in detail.

1. Understand your device ecosystem

The first step towards better security is identifying and understanding the nuances of the Wi-Fi routers you are deploying at an underlying level.

Know your CPE operating system and codebases

Today's products contain many core elements, and it is essential to know which components and libraries you are using. Many vendors in the device market build on existing distros, whether they are custom made by SoC vendors, or developed as open-source projects.

Some common open-source router distros include OpenWRT, DDWRT, prplWRT, RDK, and others. These distros rely on several additional open-source components such as OpenSSL, Apache or nginx, and even the Linux kernel itself. Often, security concerns and issues are first reported at the individual project level before distros are updated.

Consider all aspects of your device's architecture. How old is the operating system and kernel? How often does it get patched? Has it reached end-of-life and is no longer supported? All of these are essential things to understand about your CPE.

Know your interfaces and default settings

It's become clear that most Wi-Fi router vulnerabilities arise from the exploitation of default settings or from unused features and protocols that are active. Many of these features are older and have known weaknesses, or won't be used by your subscribers. These are details such as:

- What services and applications do your CPE use?
- What ports are open by default on the LAN and the WAN?
- How is the GUI accessed, and what settings are configurable?

These features affect your CPE's overall attack vectors, so be aware of these settings and what they mean for your deployed devices.

2. Require best practices

Understanding your device ecosystem is easier if you can put firm requirements on your vendors and developers to observe security best practices when it comes to Wi-Fi router design. Building these requirements into your design specifications ahead of time will make security validation much easier later on and is an integral part of your overall security process.

As we discussed above, many vulnerabilities result from common design pitfalls that make for insecure products. These pitfalls often arise from trying to balance security with ease-of-use features, or "kitchen sink design" that attempts to include as many available features as possible. Here are some of these pitfalls and the best practices used to avoid them.

Password Security

Require your vendors to use a default username and password for the user interface that is unique to each device. Moreover, ensure that access to the UI on the WAN is disabled by default.

The use of a default, well-known username and password for all of your deployed devices (like "admin" and "password") is one of the most common attack vectors of all time. For years, CPE devices have used canned passwords and made the end users responsible for changing them, which most end users never do. Attackers rely on lists of known default credentials to easily access the interfaces of deployed devices.

More devices are moving towards safer methods of accessing the user interface, such as through a smart-phone application or removing user-access altogether and relying entirely on service provider management. Even so, the importance of unique passwords applies to default Wi-Fi networks and the user interface.

Unique passwords can be provided in firmware (perhaps printed on the serial number label) or configured using your CPE management system. Using strong password practices adds even better security.

This practice is so crucial to network security that it has become part of regional regulatory requirements. Deploying devices that reuse default passwords may violate regulatory compliance.

Wi-Fi Security

Besides following the password guidelines above for default Wi-Fi networks, require that your devices use the highest level of Wi-Fi security by default and provide network separation capabilities out-of-the-box.

Despite advances in Wi-Fi security, older, legacy protocols are often retained by vendors to make sure that the end user's devices connect. These older protocols like WEP or WPA (as opposed to WPA2 or WPA3) have been compromised for some time, and present an easy target for "wardrivers" or attackers using public hotspots.

Require that your devices use at least WPA2-Personal with AES encryption (rather than TKIP) by default, and not in mixed mode with WPA. Devices that support WPA3 are even better, but (at the time of writing this guide) may not be widely available.

In addition, it's well known that today's smart home devices are built with poor security, either because of a lack of expertise or to save on costs. Subscribers also want to isolate guests from their primary home network. Having Wi-Fi networks dedicated to specific use cases by default, or configured during the on-boarding process, will provide your subscribers with the right balance between security and ease-of-use.

Securing Cloud Communications

Require that any communications to cloud services by the CPE, or by 3rd party applications running on the CPE, use modern authentication and encryption and do not transmit sensitive user data.

During the last few years, we've seen many products come to market that attempt to solve consumer pain points in Wi-Fi coverage, stability, parental controls, or (ironically) security by offering cloud-management of various services exclusively through the manufacturer. Some began as crowd-sourced products or from start-ups looking to capture a market quickly. Others are still provided as low-cost retail alternatives to more expensive gateways.

At QA Cafe, we've tested many of these products, and what we found was alarming. Some devices would communicate with the cloud over HTTP (not HTTPS), revealing MAC addresses, passwords, etc. Others would implement TLS poorly, accepting bad certificates or ignoring credentials altogether. This allows hackers to access cloud services without credentials or to impersonate cloud services to steal information.

When using TLS, don't use implementations older than TLS 1.2. Additionally, avoid deprecated, compromised cipher suites. Your CPEs absolutely must be configured to validate certificates for any cloud services they are connected to.

These requirements stand for your management systems as well. Though protocols like TR-069 are secure, they are often not deployed with well-validated security, or are entrusted to run in walled-garden networks. Criticism of cloud management from the security and privacy communities usually amounts to criticism of poorly secured management systems rather than insecure protocols.

No UPnP! (and other unnecessary services)

Require that your CPE run only the services necessary to function correctly. Require that they run with minimal permissions and that all unnecessary ports are closed. Most importantly, don't allow the Universal Plug-n-Play (UPnP) protocol by default.

UPnP is a protocol for onboarding and controlling many home networking devices and applications. It is older, and many UPnP implementations are plagued with vulnerabilities. A search of UPnP in the CVE (Common Vulnerabilities and Exposures) database currently turns up 80 different CVEs[1].

UPnP is one of the biggest offenders, but you should require that your CPE limit the number of services it runs as much as possible. Services like FTP, Telnet, Samba, etc. are often switched on for feature-rich gateways but are not valuable to the average user and dangerous to leave running.

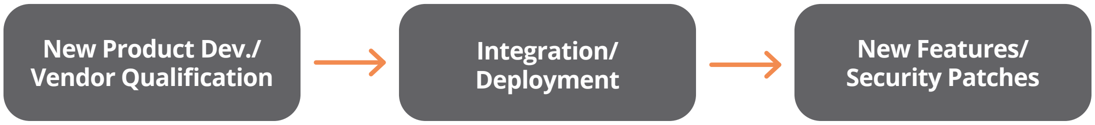
For those services that are necessary, ensure that they run according to the "principle of least privilege." That is, no services should be running as root.

Lastly, make sure that you have a good understanding of the ports that a device leaves open by default and get them to close (in stealth mode) any that aren't explicitly needed. Open TCP or UDP ports on the WAN are an instant way to fail any security verification checks. Open ports on the LAN are considered vulnerable attack points, especially in the age of the Internet of Things devices.

[1] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=upnp

3. Test, Test, Test

The best way to guarantee the security of the products you deploy is consistent testing at all stages of the CPE life cycle.


New Product Dev./ Vendor Qualification
Integration/ Deployment
New Features/ Security Patches

The CPE Lifecycle

Security touches all testing aspects, such as verifying firewalls and parental controls, checking for known vulnerabilities, stress testing, performance testing, validation of configurations, and code inspection. Just about every development and test process can be evaluated from a security perspective. Think of this as a process goal and understand how all your test activities impact security.

Active scanning

Testing your CPE's security profile starts with using tools to discover how vulnerable they are and how they appear on a network to would-be attackers. This is accomplished by automating network discovery/security audit tools (sometimes referred to as "port scanning") to see which ports and services are open by default on your CPE, and what an attacker can learn about its operating system and other information.

The most popular tool for port scanning is Nmap ("Network Mapper"), a free and open-source utility for network discovery and security auditing. Nmap uses raw IP packets to determine what services your CPE are offering, what operating systems they are running, what type of packet filters/firewalls are in use, and more. Include automated nmap scans as a baseline for any security testing of your CPE.

The CDRouter Security add-on includes a fully automated set of tests that use Nmap to probe your device under test in several ways. Use the nmap, nmap-wan, and their IPv6 counterparts as a starting point for any security test package.

It is challenging to balance ease of use with security, especially when security measures get in the way of testing and development. Test engineers often disable security measures, run services as root, or use other weak passwords to make their processes more manageable. Ensure that these shortcuts don't end up in production firmware!

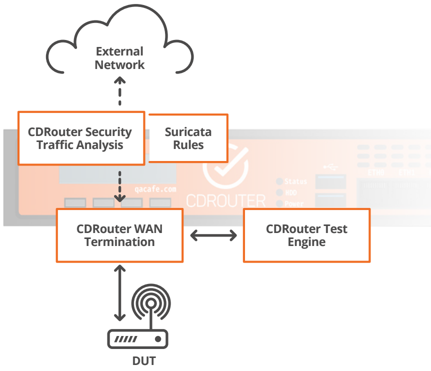
Passive monitoring

In addition to actively testing known vulnerabilities, port scanning, and exercising security features, monitoring your products' live network behavior can reveal security flaws and outline best practices critical to product quality, reducing future design changes or compromised customer networks.

Performing security traffic analysis during testing lets you observe your devices' behavior outside of the known and predictable test traffic. By monitoring the traffic a CPE sends to the Internet or specific cloud resources, you can receive alerts for suspicious, surprising traffic or behavior that goes against your deployment policy guidelines.

These alerts work alongside traditional pass/fail results or performance metrics. Often, we've seen alerts triggered by traffic sent by the device due to simulated user activity like web traffic, DNS queries, etc. These alerts let you get a full picture of your device's real-world behavior.

CDRouter's Security add-on includes a unique traffic monitoring feature that analyzes any network data your device is sending to the live network. It has standardized alerts from the Suricata traffic monitoring system, best-practice rules curated by the experts at QA Cafe, and the ability to write your own alert rules specific to your policy guidelines.



Passive traffic monitoring during testing

Validating security features

It's promising that more CPE are adding robust security and privacy features to their devices. In addition to basic firewall functionality, these include applications like DNS over TLS/HTTPS, device fingerprinting, traffic monitoring with cloud-based intelligence applications, and network management features like parental controls.

Testing that these applications work, and work well, should be included in your overall security test process. In particular, validate features that rely on cloud-based communications to prove that they do not fail or pass sensitive information in a way that can be compromised.

Additionally, test network features like guest Wi-Fi networks to ensure that traffic does indeed stay on the appropriate network. Also make sure to test advanced features including VPN tunneling, VLANs, etc.

CDRouter's Security add-on contains dozens of test modules for validating your CPE's security, privacy, and network applications.

Regular regression testing

Regression testing is perhaps the biggest use case for automation. Every change made to a CPE's firmware can affect other features, services, performance, and stability. Ensuring that security patches fix issues and do not undo any previous fixes is critical to your deployment's overall success.

Repeatability is at the heart of regression testing. Eliminate as many variables as possible with consistent, standardized test cases that are run consistently from one firmware to the next. Automate this testing alongside your continuous integration (CI) system to reduce the number of human errors.

Additionally, testing your downgrade path is equally vital to testing each firmware update. Make sure that changes can be rolled back safely without opening new issues.

CDRouter is an ideal tool for regression testing of all CPE features. Its thorough and easy-to-use API works well with CI tools like Bamboo and Jenkins for consistent, repeatable testing that eliminates manual testing variability.

Application protocols and code/shell injection

For applications that communicate information at the application level (over a REST API or other session-based protocol) should be tested rigorously for code injection flaws.

For example, the Mirai worm used a shell injection technique to instruct the target to download and run malware, turning the target into a DoS participant.
A shell injection attack is a type of code injection that takes advantage of exposed services that pass arguments into a Unix based shell. If not checked for escape characters, these arguments may instead be executed as shell commands rather than passed along as they should be. For configuration protocols like TR-064 or TR-069, this means that configuration arguments ("parameters") are passed to another application to perform configuration operations. The operating system then executes the escaped command.

The most important thing you can do to prevent these issues is to perform rigorous data validation on the Remote Procedure Calls (RPCs) used in any configuration protocol, such as TR-069, USP, SNMP, NETCONF, or proprietary web API functions.

CDRouter contains test cases for several known zero-day code injection attacks, including the so-called TR-069 Mirai vulnerability. In addition, its management protocol test cases include easy-to-customize "Scenario" test cases to develop your data-validation testing.

Long-term stability

Testing for vulnerabilities and features alone is only part of the overall security strategy in developing your CPE. It's also important to test your device's performance in the face of long-term heavy usage and its ability to handle large amounts of clients and connections. Devices may have code flaws that, when under stress, can suffer from fragmentation and memory leaks that can crash an application (possibly allowing root access to the device). System-level issues involving memory can also lead to complete system failure.

Most devices contain OS and application level diagnostics that help expose memory fragmentation and leak issues. Run these diagnostics during automated testing to get an understanding of the type and severity of issues your CPE may have. Running performance tests alongside protocol validation and client simulation will also give you a picture of the long-term stability of your CPE—some CPE see a severe degradation in performance after heavy use due to these issues.

Include some long-term stability and scalability testing as a stage in your security test process. Looping repeated tests for hours or days can expose flaws that regular testing may not bring to light.

CDRouter's Performance add-on and client scalability features specifically cover these scenarios. Most "packet blasting" performance tools don't exercise the basic functions of a CPE in tandem, missing stability issues that could result in security flaws.

Don’t forget about IPv6

IPv6 is a reality and used in many service provider deployments, most often with IPv4/IPv6 coexistence (“transition”) mechanisms like DS-Lite, lw4o6, 6rd, MAP-T, and MAP-E.

Many existing exploits work over both IPv4 and IPv6. As such, test any CPE functionality over both IPv4 and IPv6 connectivity. Firewalls and other security features may have been tested and are working over IPv4, but some implementations have flaws where the same behavior won’t work over IPv6.

For example, when fingerprinting your device using Nmap, make sure ports are closed over both IPv4 and IPv6. If IPv6 is disabled completely, make sure it actually has been disabled!

CDRouter is built for both IPv4 and IPv6 enabled devices, and contains a full suite of test cases that cover all manner of functionality over both protocols. In addition, it contains exhaustive test cases for validating your CPE’s implementation of IPv6 transition mechanisms.

4. Work with your vendors

Deploying secure devices hinges on good development practices. When your CPE are developed by a third party, these practices must become part of your overall relationship with your vendor. Clear requirements, repeatable testing, and effective feedback are crucial during the entire lifecycle of your CPE.

Have a strategy for CPE lifecycle

Though there are many steps you can take to reduce the likelihood of vulnerabilities, work with your vendors on an upgrade strategy, support window, and obsolescence plan for your CPE. Ultimately, when a security issue is discovered, your ability to quickly patch device firmware and deploy the update to your install base will mean the difference between a simple flaw and a newsworthy breach that affects thousands of devices.

Also have a process for discovering CVEs in your CPE’s underlying components and coordinating on them with your vendors. Important questions to ask include: What do you do when they are discovered? How and where are they reported? How do your vendors alert you of potential vulnerabilities? How do they work with their OEM or SoC partners? Keeping communication open will help mitigate the damage.

Duplicate your test setup

Agile development processes extend to your entire supply chain. It’s especially important for security, as it keeps the lines of communication open and ensures that security flaws are discovered and fixed quickly. Having redundant test processes between your team and your vendors reduces the variables and human error that can make security issues much worse than they need to be.

To make this effective, work with your vendors to use the same test setup as you do, with the same equipment, test cases, and automation. Let them know which tests are most important to you, and have the test packages, configurations, and run conditions closely aligned.

Share results

In addition to duplicating your overall test setup, have a process with your vendors for sharing and communicating on test results.

A duplicate test system that allows you to export test runs to preserve configuration and test case details goes far for coordinating with your vendors. Adding a process to discuss results together and share between test and development teams will make this significantly easier.

Work with the experts

Networking is complex, and it’s difficult to stay ahead of all of the different technologies, industry standards, and best practices that are critical to creating secure products. Work with trusted third-party experts in standards and security testing during your product lifecycle to stay ahead of security issues, and to resolve differences between you and your vendors. Where possible, use standardized test systems or systems that have become widely accepted and implemented by the industry.

It all starts with change

One of our team members at QA Cafe is fond of saying that security is hard, and being secure takes intent, knowledge, and effort. Security touches all parts of network and CPE design. Producing robust and secure devices requires security to be a front-facing mindset built into your entire process and CPE lifecycle.

It is understandably difficult to balance security, cost, and ease of use. Service providers are in a unique place to manage this balance and take the lead on CPE security. With the right processes in place, particularly rigorous, automated testing, you won't have to trade off as much. Taking these steps during development is critical to ensuring the safety and security of home networks, end-users, and the Internet as a whole.

The CPE Security Readiness Checklist

Use this list as a check against your CPE design and development processes. Following these steps will improve CPE security over all and protect your networks, your users, and your brand.

- ☑ We routinely review our CPE hardware and software ecosystem.
- ☑ We provide clear requirements for best practices to our vendors.
- ☑ Our vendors test for and clearly communicate security issues.
- ☑ We test for known issues and monitor our device behavior during testing.
- ☑ We have an agile process to develop, test, and deploy new firmware.
- ☑ We use automated, repeatable, standardized test tools and coordinate testing with our vendors on testing.

CDRouter by QA Cafe

CDRouter is the industry standard for testing broadband CPE and is the premier automated testing tool for security, performance, and more. We at QA Cafe want to help you build better products so you can build better networks. Better networks bring a better world for you and your subscribers.

Learn more at: www.qacafe.com/cdrouter/.

The CPE Security Readiness Checklist

The four key points to stick to when ensuring secure devices:

- □ Understand your device ecosystem.
- □ Require best practices.
- □ Make regular testing part of your process.
- □ Work with your vendors.

The CPE Security Readiness Checklist

- □ We routinely review our CPE hardware and software ecosystem.
- □ We provide clear requirements for best practices to our vendors.
- □ Our vendors test for and clearly communicate security issues.
- □ We test for known issues and monitor our device behavior during testing.
- □ We have an agile process to develop, test, and deploy new firmware.
- □ We use automated, repeatable, standardized test tools and coordinate testing with our vendors on testing.