Rethinking WiFi and Router Security: A Deep Dive into the Recent ASUS Flaw and Secure Alternatives

Dave Wreski ⋮ 12-15 minutes

At a time of rapid technological progress, the security of our digital tools - particularly WiFi routers - has become critical. Recent news from ASUS sent shockwaves through the cybersecurity community when multiple models of their routers were found with critical flaws that exposed an ongoing challenge of protecting networks against intrusions.

Unpacking the Critical Flaw in ASUS Routers

According to an extensive report by RedPacket Security, ASUS recently resolved an authentication bypass vulnerability known as CVE-2024-3080, which scored 9.8 on the Common Vulnerability Scoring System scale, indicating its severity. This security hole allowed unauthenticated, remote attackers to access devices for unauthorized gains without authentication, granting them any legitimate privileges whatsoever.

Another high-severity buffer overflow flaw, CVE-2024-3079, compounded this security hole by enabling remote attackers with administrative privileges to execute arbitrary commands remotely on devices with administrative rights. These vulnerabilities could constitute an exploit chain compromising all security protection on affected routers.

ASUS routers such as the ZenWiFi XT8, RT-AX88U, RT-AX58U, and others were affected. ASUS quickly responded with software updates to address these vulnerabilities.

This incident raises a fundamental issue regarding routers' reliance on proprietary software. While manufacturers frequently push out security patches, proprietary programs' closed nature means vulnerabilities remain unseen until a breach occurs, leaving users vulnerable.

Sign up for our newsletters and receive a your free infographic

Embracing Open Source: A Route to Enhanced Security

Open-source firmware and operating systems offer an alternative to proprietary router software. Their publicly collaborative development processes make security flaws less likely to go undetected.

OpenWRT

OpenWrt is one of the most widely used open-source router operating systems available. It provides highly configurable control over performance and security settings, surpassing what most stock router firmware allows. OpenWrt also features an innovative package management system that enables users to add or remove features as desired, making the operating system leaner and more cost-effective than others.

Here are five of the best features of OpenWrt:

- Extensive Hardware Support: OpenWrt supports a wide range of devices, from home routers to professional-grade equipment, making it adaptable to various networking situations.
- Fully Writeable Filesystem: With its roots in Linux, OpenWrt provides a fully writeable filesystem. Users can modify, add, or delete any file, similar to a traditional Linux distribution, offering unparalleled flexibility.
- Customizable Packages: OpenWrt allows users to install and remove packages to customize the router for specific needs without bloating the system with unnecessary features.
- Advanced Network Capabilities: OpenWrt contains many out-of-the-box network features, including IPv6 support, VLANs, traffic shaping, VPN, and firewall configurations, allowing for detailed network management.\
- Active Community and Development: The vibrant OpenWrt community and ongoing development mean

the firmware is constantly updated. New features are regularly added, and security vulnerabilities are promptly addressed, enhancing your network's functionality and security.

These features underscore OpenWrt's flexibility and capabilities, making it a powerful choice for users looking to maximize their router's potential.

DD-WRT

Like OpenWrt, DD-WRT is another Linux-based firmware that enhances routers by improving network stability, range expansion, and security features such as VPN integration and VLAN support. Furthermore, its community is quite active, providing resources and forums for help and advice regarding its usage.

The five best features of DD-WRT include:

- Advanced Quality of Service (QoS): This technology enables intricate control over bandwidth allocation to prioritize traffic or devices for improved network performance.
- VPN Integration: Facilitates the integration of a Virtual Private Network directly within the router, securing all connected devices without individual configuration.
- Wireless Bridge and Repeater Modes: Allows routers to function as wireless repeaters or bridges, extending the wireless network's coverage or connecting wired devices to a wireless network.
- VLAN Support: Supports Virtual LANs for better network segmentation, enhancing security and management, and is especially useful for guest or separate IoT networks.
- DNS Caching: Stores DNS queries locally to speed up webpage loading times, resulting in a faster internet experience for all network users.

Tomato

Tomato firmware is known for its user-friendly interface and emphasis on real-time network monitoring, supporting many of the same models as DD-WRT while offering more secure security features than its stock counterpart.

Here are five of the best features of Tomato firmware for routers:

- Bandwidth Monitoring: This allows users to monitor network traffic and bandwidth usage, making it easier to manage network resources effectively.
- Advanced Quality of Service (QoS) provides detailed settings to prioritize network traffic, which helps optimize performance for critical applications.
- Access Control: Offers robust options to manage and control access to the network, enhancing security by restricting unauthorized usage.
- Built-in OpenVPN Server/Client: Integrates support for OpenVPN, enabling secure VPN connectivity for enhanced privacy and secure remote access.
- IP/MAC Bandwidth Limiter: This tool enables setting bandwidth limits for specific IP addresses or MAC addresses, useful in managing bandwidth consumption per device.

These features enhance network management, security, and performance, making Tomato firmware a valuable choice for users with compatible Broadcom-based routers.

pfSense

While not specifically for routers, pfSense can transform an old computer into a powerful firewall and router. Based on FreeBSD and widely regarded as one of the safest and most flexible network administration solutions available today, pfSense handles everything from routing and firewalling to VPN provisioning easily.

Here are the five best features of pfSense router firmware:

- Comprehensive Firewall Security: pfSense provides an advanced firewall with stateful packet inspection, anti-spoofing, and more, for robust network protection.
- Versatile VPN Support: It supports multiple VPN protocols, including IPsec, OpenVPN, and WireGuard, enabling secure and flexible remote access configurations.
- High Availability and Redundancy: This service offers features like CARP (Common Address Redundancy Protocol) and pfsync to ensure network uptime and reliability through failover and redundancy setups.

- Traffic Shaping and QoS: This allows detailed control over network traffic, enabling the prioritization of critical services to maintain optimal performance and reduce congestion.
- Extensibility with Packages: This can be extended with a wide range of packages for additional features, such as Snort for intrusion detection, Squid for web caching, and more, tailoring the system to specific needs.

AsusWRT-Merlin: Custom Firmware Powering ASUS Routers

AsusWRT-Merlin is a third-party firmware developed for select ASUS routers by Eric Sauvageau to improve upon the original AsusWRT firmware without drastically altering its user experience or user interface. Retaining all original features while adding improvements, bug fixes, and occasional new ones;

Eric Sauvageau leads the development of AsusWRT-Merlin with support from The Merlin Group, users, and developers who contribute to its ongoing maintenance and enhancement. Their efforts focus on stability, improved performance, and better customization possibilities across ASUS router models supported by this open-source firmware project.

Using AsusWRT-Merlin can bring many advantages for users who appreciate open source's philosophy and its associated benefits:

- Improved Security: Regular updates from the Merlin Group may include security patches which make your router less susceptible to vulnerabilities discovered over time.
- Enhanced Features: The AsusWRT-Merlin includes additional features not found in its predecessor AsusWRT, such as DNS over HTTPS support (DoH), enhanced Quality of Service capabilities (QoS), and the option to monitor real-time bandwidth usage.
- Customizability Freedom: Fans looking to tailor their network according to specific needs will appreciate the various settings and tweaks available.
- Active Community Support: Our vibrant community works tirelessly on improvements and shares knowledge for troubleshooting and advanced configurations.

Open Source Firmware Limitations

AsusWRT-Merlin keeps users familiar with AsusWRT at ease since its GUI and overall design philosophy are the same as before, helping ease any learning curve. Open-source firmware such as this also comes with some restrictions users should be aware of:

- Warranty Concerns: Installing third-party firmware could void your device's manufacturer warranty; users should check their warranty terms before proceeding.
- Limited Support: While community support exists for using third-party firmware such as AsusWRT-Merlin, users will not receive official assistance from ASUS for issues caused by using such third-party solutions.
- Compatibility and Stability: Not all routers can support third-party firmware, and while open-source firmware tends to be stable, poorly executed updates or incompatible configurations could create stability issues.
- Learning Curve: For less tech-savvy, understanding all the additional features and configuration options may take more effort than familiarising themselves with stock firmware's user-friendly setups.
- No Guarantee of Features: Unfortunately, Merlin may not support all the proprietary features found in AsusWRT; some features present may also sometimes be removed if they pose significant bugs or security risks.

Although open-source firmware such as AsusWRT-Merlin may have disadvantages, many advanced users find the advantages far outweigh them, particularly its enhanced control and security features. Individuals looking to maximize the potential of their router will discover that this version provides a robust upgrade from the original AsusWRT, offering both familiarity with stock firmware and access to more sophisticated capabilities of fully open-source solutions.

Sign up for our newsletters and receive a your free infographic

Making the Switch to Open-Source Firmware for Enhanced

Network Security

Transitioning to open-source firmware like AsusWRT-Merlin can be an important strategic move for users who prioritize network security. However, this endeavor must be carefully prepared to ensure a successful transition.

Before making the change, you must verify whether or not the open-source firmware you've selected is compatible with your router model. Not all routers support all firmware installations; installing incompatible ones could result in functional severe issues or even brick your device. Once compatibility has been confirmed, backing up existing router settings as a protective measure can prevent data loss and help ensure smooth transition processes.

As installation processes can differ between router models, it is wise to refer to an after-installing guide tailored specifically for your router model for after-installation instructions and potential obstacles related to firmware upgrading processes. Such guides often offer step-by-step guidance and can help address common obstacles encountered during this process.

The Bigger Picture

The ASUS incident highlights the need for more proactive security measures in network hardware. By turning to open-source solutions, users can take advantage of collective approaches to security where vulnerabilities can be quickly identified and patched by an international community of developers.

Transitioning to open-source software might initially appear daunting; however, spending the time and energy learning how to utilize these powerful tools can significantly boost both the security and efficiency of home or office networks.

Open source network management represents more than software changes; it represents a wider trend toward transparency and community in cybersecurity—an essential aspect in today's increasingly interconnected society.