**Adventures in IoT Hacking Referenced Article Links**

National Vulnerability Database​

https://nvd.nist.gov​

Search on: TP-Link Router TL-WR841N

OWASP

https://owasp.org/blog/2024/03/01/iot-security-testing-guide.html​

This guide aims to provide comprehensive insights into testing the security of IoT devices and systems.

IOT Attacks in History

Mirai Botnet circa (2016 - today)​

https://en.wikipedia.org/wiki/Mirai\_(malware)​

https://www.infosecurity-magazine.com/news/mirai-botnet-zerodays-routers/​

BrickerBot (2017)​

https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/​

Silex (2019)​

https://www.bleepingcomputer.com/news/security/new-silex-malware-trashes-iot-devices-using-default-passwords/ ​

Eleven11bot (2025)​

<https://www.bleepingcomputer.com/news/security/new-eleven11bot-botnet-infects-86-000-devices-for-ddos-attacks/>

shadowserver.org map of “Eleven11Bot”

More recent IoT attacks

* <https://cybersecuritynews.com/hackers-exploiting-tp-link-vulnerability/#webview=1>​

*critical vulnerability in TP-Link TL-WR845N routers that could allow attackers to gain complete control over affected devices* credentials are stored in two specific locations: “squashfs-root/etc/passwd” and “squashfs-root/etc/passwd.bak”. The exposed hardcoded root password can be easily cracked to reveal “1234” while the root username appears in plaintext as “admin.”​

* <https://www.securityweek.com/edimax-says-no-patches-coming-for-zero-day-exploited-by-botnets/#webview=1>​

*Edimax explained. “Due to the unavailability of the development environment and source code, we regret to inform that no security patch or firmware update can be provided for this product.”*​

* <https://www.securityweek.com/unpatched-edimax-camera-flaw-exploited-since-at-least-may-2024/>​

*The vulnerability, identified as CVE-2025-1316, has been confirmed to impact Edimax IC-7100 IP cameras, but Akamai believes other Edimax IoT products may be impacted as well.* ​

* <https://www.tomsguide.com/computing/malware-adware/thousands-of-tp-link-routers-have-been-infected-by-a-botnet-to-spread-malware>​

*TP-Link Archer AX-21 router...was used in the* [*Mirai botnet*](https://www.tomsguide.com/news/android-adb-matryosh-botnet) *malware attacks. The flaw also linked to the Condi and AndroxGh0st malware attacks*​

* <https://arstechnica.com/security/2025/03/massive-botnet-that-appeared-overnight-is-delivering-record-size-ddoses/>​

*Yet another, even larger, “Eleven11Bot” attack March 6, 2025*