

Sources utilized to conduct static and dynamic analysis of Wi-Fi router firmware.

1. Asus – RT AX55
 - a. https://www.asus.com/networking-iot-servers/wifi-routers/all-series/rt-ax55/helpdesk_bios?model2Name=RT-AX55
 - b. <https://www.tomsguide.com/news/these-asus-routers-are-vulnerable-to-remote-code-execution-flaws-update-right-now>
 - c. <https://nvd.nist.gov/vuln/detail/CVE-2023-39780>
 - d. https://dlcdnets.asus.com/pub/ASUS/wireless/RT-AX55/FW_RT_AX55_300438651598.zip?model=RT-AX55
2. TP-Link WR841N
 - a. <https://www.tp-link.com/us/support/download/tl-wr841n/>
 - b. <https://medium.com/tenable-techblog/drive-by-exploiting-tp-link-routers-a3ef7b31c004>
 - c. <https://www.tenable.com/security/research/tra-2018-27>
 - d. <https://github.com/adamhlt/TL-WR841N>
 - e. https://nahueldsanchez.com.ar/Playing-with-a-TP-LINK-TR841_II/
3. D-Link DIR-860L
 - a. <https://legacyfiles.us.dlink.com/DIR-860L/REVB/FIRMWARE/>
 - b. <https://github.com/musashino205/lede-source/blob/master/target/linux/ramips/dts/DIR-860L-B1.dts>
 - c. <https://sourceforge.net/projects/ddwrtdir860l/files/Firmwares/>
 - d. <https://github.com/lembang/dd-wrt-dir860l>