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

1. TP-Link WR940N
    a. https://github.com/b1ack0wl/vulnerability-write-ups/blob/master/TP-Link/WR940N/112022/Part1.md
    b. https://www.exploit-db.com/exploits/43022
    c. https://www.tp-link.com/ca/support/download/tl-wr940n/v3/#Firmware
    d. https://www.tp-link.com/ca/support/download/tl-wr941nd/#Firmware
2. Belkin N300
    a. https://nvd.nist.gov/vuln/detail/CVE-2013-3089
    b. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3090
    c. https://www.zerodayinitiative.com/advisories/ZDI-15-343/
    d. https://www.zerodayinitiative.com/advisories/ZDI-15-346/
3. Netgear WNAP320
    a. https://faisalfs10x.github.io/thm/IoT#
    b. https://www.netgear.com/support/product/wnap320
    c. https://nvd.nist.gov/vuln/detail/CVE-2022-31876
    d. https://www.exploit-db.com/exploits/50069
    e. https://www.exploit-db.com/exploits/46678