Resources used for Reference:

- Automated Security Analysis of Firmware by Farrokh Bolandi
  Information and Communication Technology
  KTH Royal Institute of Technology
  Stockholm, Sweden
- https://prabhankar.medium.com/firmware-analysis-part-1-cd43a1ad3f38
- https://en.wikipedia.org/wiki/Zero-day_(computing)
- https://www.cloudflare.com/learning/dns/glossary/dynamic-dns/

D-Link:

- https://support.dlink.com.au/Download/download.aspx?product=DIR-882
- https://hackaday.com/2020/08/24/hacking-d-link-firmware/
- https://www.pcworld.com/article/419842/new-firmware-analysis-framework-finds-serious-flaws-in-netgear-and-d-link-devices.html

Linksys:

- https://www.linksys.com/gb/support-article/?articleNum=47131
- https://www.opencve.io/cve/CVE-2022-38132
- https://www.linksys.com/support-article?articleNum=246427

Netgear:

- https://www.netgear.com/support/product/r6250#download
- https://bryanleong98.medium.com/firmware-analysis-on-netgear-access-point-wnap-320-20ab7e67ea7e
- https://news.ycombinator.com/item?id=23537388