UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00143

WI-FI RESEARCHER UNCOVERS "FRAGATTACKS"

DATE ISSUED: 17th May 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Short for "Fragmentation and Aggregation Attacks" – FragAttacks have been discovered by a Belgian researcher (who also discovered the KRACK attack possible with WPA2) that hark back to 1997 enabling a range of devices to become compromised if they are in Wi-Fi Range allowing data interception, full device takeover and execution of malicious code.

BREAKDOWN

Three of the vulnerabilities discovered in the FragAttacks family are due to design flaws in the Wi-Fi standard meaning most devices are affected while others are attributed to widespread programming mistakes. What this means is that all devices used in the study were affected by at least one of these vulnerabilities. The flaws are not under known active exploitation at present and while they would be difficult to uncover, if exploited could cause a "perfect storm" and affect masses of users and Wi-Fi capable devices. The recent announcement has been made after a none-month embargo was lifted, during which time the Wi-Fi Alliance has been making major changes to their standards and guidelines and working with vendors to release a series of security patches.

REMEDIATION STEPS

- Install vendor security patches for Wi-Fi capable devices as soon as they become available – check devices that don't get updated regularly including IoT (Internet of Things) devices.
- Keep passwords unique and change default passwords on IoT and network devices.
- Use URL filtering to prevent access to known or suspicious websites. Check sites being visited are using HTTPS and configure your DNS to prevent poisoning.
- Use the tool available on GitHub (see resource below) supplied by the aforementioned research team to test vulnerabilities in Wi-Fi access points.
- Remove any Wi-Fi devices that are using WEP as a security protocol and switch to WPA2 capable devices.
- See full list (provided in Threatpost resource) to check device change logs for updates relating to the appropriate CVE's listed.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/fragattacks-wifi-bugs-millions-devices/166080/
GitHub https://github.com/vanhoefm/fragattacks
ZDNet https://www.zdnet.com/article/time-to-patch-against-fragattacks-but-good-luck-with-home-routers-and-iot-devices/