Are SURFboard products affected by FragAttack Vulnerability?

ARRIS (owned and operated by CommScope) is committed to the security of our devices and the millions of customers who use our products.

The FragAttacks vulnerabilities were publicly disclosed on May 11, 2021, by the Wi-Fi Alliance. These vulnerabilities may allow an adversary to forge encrypted frames, allowing exfiltration of any data transmitted over a Wi-Fi link. All devices using the Wi-Fi protocol (802.11) are affected.

ARRIS and CommScope takes all vulnerabilities seriously. We are assessing applicability to our products, and where necessary, developing firmware patches and evaluating other mitigation approaches to minimize the potential impact of FragAttacks vulnerabilities. We employ proactive security measures with our customers to minimize the impact of broad security threats like FragAttacks that aim to expose vulnerabilities in devices and networks.

Further information is available at:

- Wi-Fi Alliance: https://www.wi-fi.org/security-update-fragmentation
- Researcher's paper: https://papers.mathyvanhoef.com/usenix2021.pdf

Q&A:

What is FragAttacks vulnerability?

- This man-in-the-middle (MITM) attack can be used to manipulate and inject 802.11 frames over the air. If the WLAN AP device cannot detect such manipulation, the hacker can possibly inject malicious data or commands for that device to perform later, either immediately or possibly even minutes after successful injection.
- The FragAttacks vulnerability requires the hacker to be in range of the victim's WLAN and be in the MITM position to be able to manipulate and inject frames, in addition to the occasions where a social engineering aspect is also involved. While the research discloses the tools and methods used to discover the vulnerabilities, these are not simple attacks to carry out.
- While still impactful and needing to be remediated, there is no expectations to see a rash of these attacks. To be successful, the hacker would need to be sophisticated, onsite, and armed with specialized hardware with specific drivers. Some of the vulnerabilities rely on both MITM and social engineering being successful to exploit.
- At the technical level, this is a vulnerability with exploitation of network traffic management by a hacker. This vulnerability is like many other vulnerabilities being discovered daily in the software that we all use.
- The FragAttacks vulnerability requires the adversary to be in range of the victim's WLAN and be in the MITM position.

When did ARRIS learn about the FragAttacks vulnerability?

- The Wi-Fi Alliance publicly disclosed the FragAttacks vulnerability on May 11, 2021.
- As soon as we learned of this latest vulnerability, we took the issue very seriously and began assessing applicability to our products, and where necessary, developing firmware patches. We also evaluated other mitigation approaches to minimize the potential impact of FragAttacks vulnerabilities.

- All devices that use the Wi-Fi protocol (802.11) are susceptible to this FragAttacks vulnerability. We are informing operators and service providers of affected products and software releases that will remediate this issue.

What ARRIS SURFboard products are affected?

- We evaluated our full portfolio and the following products are impacted:
    - ARRIS SURFboard DOCSIS gateways
        - SBG10
        - SBG6950
        - SBG7400
        - SBG7600
        - SBG8300
        - SVG2482
    - ARRIS SURFboard mAX Whole-Home Wi-Fi products
        - W131/W31 mAX Pro Router
        - W130/W30 mAX Plus Router
        - W121/W21 mAX Router
        - W122 mAX Express Router

Is this issue limited to ARRIS products?

- No, this is an industry-wide issue, and the vulnerability affects all products using the Wi-Fi 802.11 protocol.

What are some of the acts that a hacker could do with FragAttacks vulnerability?

- These attacks are not easily carried out. Most require a combination of being able to inject 802.11 frames, successfully complete a MITM attack, and successfully socially engineer the victim into bypassing browser warnings about a link or to visit a site hosted by a malicious server.
- For all the above to succeed, the hacker would need to be sophisticated, within your home network's Wi-Fi range, and armed with specialized hardware and software, none of which is currently known to be publicly available. To date, there is no report of FragAttacks being carried out successfully anywhere except in a research environment.
- A hacker could use this vulnerability as a springboard to launch additional attacks that may be more likely to succeed when leveraging the compromised network.
- The FragAttacks vulnerabilities may allow an adversary to forge encrypted frames, allowing exfiltration of any data transmitted over a Wi-Fi link. This means they could intercept IP-based traffic and that a hacker could poison the cache and exfiltrate a person's data from their network.

When will a solution/firmware update be available?

- ARRIS is working with our Wi-Fi SoC vendors for patches we can distribute. An update will be provided when the firmware is available.

Will ARRIS devices in the field become worthless? Will they need to be discarded?

- No, the devices will not become worthless, but they will be vulnerable to this attack if not upgraded. This Wi-Fi vulnerability can be fixed by a downloadable software patch.

Is there a way for SURFboard consumers to protect themselves before a solution/firmware update is ready or further protect themselves from other security attacks?

- We recommend the following to our customers:
    - Update personal computing devices (i.e., laptops, mobile phone, tablets etc.) and IoT devices (i.e., smart homes, smart security devices, cameras etc.) to the latest available software versions to ensure that the most-recent fixes for bugs and security vulnerabilities are installed.
    - Update anti-virus and anti-malware software and associated definition files on personal computing devices (i.e., laptops, mobile phone, tablets etc.).
    - Use HTTPS protocol to connect to web sites, which adds another layer of encryption to data transmitted. Be aware of Social Engineering methods that ask users to click on links or navigate to unknown websites.

How can an end user tell if he/she has received a security update and his/her device is now safe?

- ARRIS is working with our Wi-Fi SoC vendors for patches we can distribute. An update will be provided on this site to include timing of the firmware release and the firmware version number for the affected products.