The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
05/12/2021

SUBJECT:
Multiple Vulnerabilities in Wi-Fi Enabled Devices Could Allow for Data Exfiltration

OVERVIEW:
Multiple vulnerabilities have been discovered in Wi-Fi enabled devices, the most severe of which could allow for data exfiltration. IEEE 802.11 is part of the IEEE 802 set of local area network technical standards, and specifies the set of medium access control and physical layer protocols for implementing wireless local area network communication. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to exfiltrate user data.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild. A proof of concept exists for various vulnerabilities mentioned within this advisory.

SYSTEMS AFFECTED:
- Any Wi-Fi enabled device could be vulnerable, please check with the manufacturer of your device(s)

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Wi-Fi enabled devices, the most severe of which could allow for data exfiltration. These vulnerabilities can be exploited if a user connects to a rogue access point and is then redirected to or visits a malicious server. Details of the vulnerabilities are as follows:

- A vulnerability exists in the 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) that could allow an attacker to inject arbitrary network packets (CVE-2020-24588)
- A vulnerability exists in the 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) that could allow an attacker to decrypt selected fragments when another device sends fragmented frames. (CVE-2020-24587)
- A vulnerability exists in the 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) that could allow an attacker to inject arbitrary network packets and/or exfiltrate user data. (CVE-2020-24586)
- A vulnerability exists in Samsung Galaxy S3 i9305 4.4.4 devices that could allow an attacker to inject arbitrary network packets independent of the network configuration. (CVE-2020-26145)
- A vulnerability exists in Samsung Galaxy S3 i9305 4.4.4 devices that could allow an attacker to inject arbitrary network packets independent of the network configuration. (CVE-2020-26144)
- A vulnerability exists in the ALFA Windows 10 driver 6.1316.1209 for AWUS036H that could allow an attacker to inject arbitrary data frames independent of the network configuration. (CVE-2020-26140)
- A vulnerability exists in the ALFA Windows 10 driver 1030.36.604 for AWUS036ACH could allow an attacker to inject arbitrary data frames independent of the network configuration. (CVE-2020-26143)
- A vulnerability exists in the kernel in NetBSD 7.1 that could allow an attacker to launch denial-of-service attacks against connected clients and makes it easier to exploit other vulnerabilities in connected clients. (CVE-2020-26139)
- A vulnerability exists in Samsung Galaxy S3 i9305 4.4.4 devices that could allow an attacker to exfiltrate selected fragments. (CVE-2020-26146)
- A vulnerability exists in the Linux kernel 5.8.9 that could allow an attacker to inject packets and/or exfiltrate selected fragments (CVE-2020-26147)
- A vulnerability exists in the kernel in OpenBSD 6.6 that could allow an attacker to inject arbitrary network packets, independent of the network configuration. (CVE-2020-26142)
- A vulnerability exists in the ALFA Windows 10 driver 6.1316.1209 for AWUS036H that could allow an attacker to inject and possibly decrypt packets. (CVE-2020-26141)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to exfiltrate of user data.

RECOMMENDATIONS:
The following actions should be taken:
- Apply the stable channel update provided by the vendor to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Wi-Fi Alliance:

https://www.wi-fi.org/security-update-fragmentation

FragAttack:
https://www.fragattacks.com/#beingexploit

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24588
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24587
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24586
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26145
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26144
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26140
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26143
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26139
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26146
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26147
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26142
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26141

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.