Honeywell

Productvity Solutions and Services
9680 Old Bailes Rd
Fort Mill, SC 29715
www.honeywell.com

Cyber Security Update

Security Notification – Wi-Fi Vulnerabilities (FragAttacks)

Background

Security researchers have reported a collection of new security vulnerabilities, FragAttacks (fragmentation and aggregation attacks), that affect Wi-Fi devices. An adversary that is within range of a victim's Wi-Fi network can abuse these vulnerabilities to steal user information or attack devices. The discovered vulnerabilities affect all modern security protocols of Wi-Fi, including the latest WPA3 specification. Even the original security protocol of Wi-Fi, called WEP, is affected. The design flaws are hard to abuse because doing so requires user interaction or is only possible when using uncommon network settings.

Recommended Action

Honeywell recommends that, subject to each customer's individual assessment of the potential impact(s) of the vulnerabilities and/or recommendations on their specific operational network environment(s), customers with potentially affected products take the following steps to mitigate the effects of potential vulnerabilities:

- Educate your users. Most attacks could be spotted by the users if the users are educated on IT security. It can be important to educate your users and introduce them to social engineering and phishing attacks.
- Implement a WIDS. A Wireless Intrusion Detection System can help us detect Rogue and Honeypot access points that an attacker could use to perform a man-in-the-middle attack. Most vendors have similar systems available. The key is to configure the WIDS properly, so it doesn't provide false positives and alerts when needed.
- Use 802.11w (when possible). 802.11w or Management Frame Protection allows some management frames to be protected. This protects the Wi-Fi network against an attacker that would want to disconnect Wi-Fi clients to start a man-in-the-middle attack.
- Use 802.1X authentication (when possible). WPA2-Enterprise of WPA3-Enterprise can be used to perform 802.1X authentication. Some of the popular EAP methods (EAP-PEAP and EAP-TLS) allow us to perform mutual authentication between the client and the server which minimize the possibility for man-in-the-middle attacks.
- Patch all your Wi-Fi devices. This includes both access points and client devices. Honeywell will release software updates to include security fixes as they are made available in partnership with our suppliers. Updates will be made available at https://hsmftp.honeywell.com, or through your Honeywell product support channel. Contact Honeywell Tech Support for more info.
- Subscribe to receive notification of Android patch availability from Honeywell by visiting the link here: https://now.honeywellaidc.com/2018-GDPR-Website-Implementation_Sign-Up-page.html?marketobu=HSM