Cambium Networks™

Unit B2, Linhay Business Park, Eastern Road
Ashburton, Devon, United Kingdom, TQ13 7UP

1 May 2023

Re: **Framing Frames: Bypassing Wi-Fi Encryption by Manipulating Transmit Queues**

Cambium Networks is investigating the issues covered in the paper recently made available at https://papers.mathyvanhoef.com/usenix2023-wifi.pdf, and so far can confirm

- Cambium cnPilot® Enterprise, Enterprise Wi-Fi 6 and Xirrus® APs are not vulnerable to the leaking of buffered frames proposed by the paper.
- The paper also describes a scenario where an attacker with valid network credentials spoofs the MAC address of the victim and overrides its security context. As noted in the paper, the default attack is limited, but they also describe a fast (re)connection attack which is feasible when two APs in the same layer 2 domain cache different versions of the PMK associated with a MAC address. Cambium's distributed control plane architecture ensures that all APs in such a network synchronize their PMK caches. Hence cnPilot® Enterprise, Enterprise Wi-Fi 6 and Xirrus® APs are not vulnerable to this fast (re)connection attack.
- We agree that IEEE standards allow ways to mount denial of service or MAC spoofing attacks as described in the paper. We will follow updates to the spec for mitigations. Meanwhile we encourage our users to follow industry best practices to reduce the impact of these and other attacks by
  - Enabling 802.11w for Management Frame Protection
  - Using upper layer security such as TLS and IPSEC
  - Using separate WLANs for internal, guest and IoT networks and mapping them to different VLANs

In addition, Cambium Networks ePSK feature allows different users on the same WLAN to be assigned their own individual VLAN, preventing the attacks described.

For questions about this notice, please email us at security@cambiumnetworks.com.

Security Team

Cambium Networks™
3800 Golf Road, Suite 360
Rolling Meadows, IL 60008