WiFi Protocol Vulnerability Exposing Network Traffic

Research has revealed that the Cisco Wireless Access Point products and Cisco Meraki products with wireless capabilities have a vulnerability in the WiFi protocols built-in power save mechanism that could allow an adversary to meddle with traffic, client connections, and more. The vulnerability lies in the 802.11 standards, which lacks appropriate security contexts for buffered frames when a receiving device is in sleep mode. When a receiving device enters sleep mode, an adversary could trick the system to grant access into leaking frames in plaintext. Additionally, a threat actor could manipulate the WiFi frames or encrypt frames before queuing or cause a denial-of-service attack utilizing this method.
The researchers that discovered this vulnerability published the exploit code on GitHub as a MacStealer tool. Cisco is aware of the vulnerability and has recommended that organizations restrict network access and encrypt data in transit whenever possible. These steps would render the acquired data unusable by the attacker. Currently, there is no known exploitation of this vulnerability in the wild.
Organizations should ensure their network admins are restricting network access and that employees are encrypting data in transit, such as internal and external emails. If data in transit is not encrypted, this can result in sensitive corporate data being stolen. We recommend organizations provide education and training to their employees on new vulnerabilities and how to mitigate them.

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the situation and work closely with the Threat Detection Engineering (TDE) team and the SOC to implement any relevant detections. For future updates, the CTI team will post via ZTAP® Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wifi-ffeb-22epcEWu
2. https://latesthackingnews.com/2023/03/31/study-reveals-wifi-protocol-vulnerability-exposing-network-traffic/