Security Advisory

- CVE-2019-9494
- CVE-2019-9495
- CVE-2019-9496
- CVE-2019-9497
- CVE-2019-9498
- CVE-2019-9499

The Wi-Fi Alliance has notified its members of vulnerabilities (CVE-2019-9494, CVE-2019-9495, CVE-2019-9496, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499) in a limited number of early implementations of WPA3-Personal™ where those devices allow collection of side channel information on a device running an attacker's software, do not properly implement certain cryptographic operations, or use unsuitable cryptographic elements. WPA3-Personal is in the early stages of deployment, and the small number of device manufacturers that are affected have already started deploying patches to resolve the issues. These issues can all be mitigated through software updates without any impact on the devices' ability to work well together.

While there is low probability of exploitation on the affected systems, Marvell places the highest priority on addressing security concerns and has deployed a fix to address this issue. We have been working closely with our customers to update Marvell's latest firmware and driver to implement the most recent security enhancements.

Marvell encourages customers to contact their Marvell representative for additional support.

Public Information:

- Wi-Fi Alliance public statement: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-security-update-april-2019
- Wi-Fi Alliance public overview website and FAQ: https://www.wi-fi.org/security-update-april-2019