Security Advisory

CVE-2019-6496

Marvell was made aware of a potential vulnerability (CVE-2019-6496), which was presented at the ZeroNights conference on November 21-22, 2018, with regard to our 88W8897 device. As Marvell places the highest priority on addressing security concerns, we immediately acted to understand the issue and implemented a fix.

In the presentation, detail was provided to manipulate the open-source Valve Steamlink platform to exploit a memory buffer overflow issue in the device firmware. Unlike this non-secure Valve Steamlink platform, the other systems mentioned in the presentation are all closed systems with high-level security protections in place such as DRM. As noted in the presenter's blog, this would eliminate the ability for an individual to compromise the system security:

> "You may notice, that the majority of devices which use Marvell Wi-Fi are gaming devices, like PS 4 (maybe because of high-performance 802.11ac and Bluetooth COMBO). It's difficult to research them because of the DRM protection."

Marvell is not aware of any real world exploitation of this vulnerability outside of a controlled environment.

Marvell deployed a fix to address this issue which we have made available in our standard driver and firmware. We have communicated to our direct customers to update to Marvell's latest firmware and driver to get the most recent security enhancements, including support for WPA3.

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