Security Advisory

Marvell was made aware of vulnerabilities in the Linux mitigation for “Spectre v2” on the ThunderX2® server platform based on research conducted by Google’s Safeside project. Marvell thanks Anthony Steinhauser of Google’s Safeside project for continued security research and appreciates the collaboration.

The vulnerability identified by Google’s Safeside project is based on the same root cause as found in the January 2018 disclosure from Marvell (then Cavium) of “Spectre v2” (CVE-2017-5715). At that time, Marvell (Cavium) in collaboration with Arm and industry partners worked to make software (firmware and OS) mitigations available and ThunderX® customers were informed of their options. At the time the software mitigations were released, validation was incomplete since the developers did not have an attack example they could validate against. Google’s recent research has exposed that the software mitigation had shortcomings. Updated versions of the software mitigation patch are available and any customers that need it should reach out to Marvell.