Security Advisory

Published: June 17, 2022

Marvell is aware of the recent PACMAN attack published by CSAIL at MIT (https://www.csail.mit.edu/news/researchers-discover-new-hardware-vulnerability-apple-m1-chip). This attack allows the discovery of the pointer authentication code (PAC) keys, effectively nullifying the additional protections PAC was intended to provide. Marvell was properly notified by Arm of this issue after discovery.

Marvell's Neoverse N2 core in CN(F)10xxx is susceptible to this attack. Other earlier CN(F)xxxx products' cores are not susceptible as they did not support PAC. Marvell's other products in production, including CN(F)9xxx products, are not susceptible as these products do not support PAC.

This attack does not provide any additional data exposure besides breaking the additional security PAC provides, therefore Marvell still views PAC as providing some additional protection as malicious code would still have the additional layer of PAC to mount a successful attack.

Marvell places the highest priority on addressing security concerns. Marvell has been working with its direct customers to provide recommended resolutions and updates from ARM. Marvell encourages customers to contact their Marvell representative for any additional support.