Security Advisory

Published: September 7, 2022

Marvell is aware of the recently published USENIX research paper shown below.

The 31st USENIX Security Symposium, August 10-12, 2022, in Boston, MA, USA included a paper “Open to a fault: On the passive compromise of TLS keys via transient errors” by Sullivan, et. al. (https://www.usenix.org/conference/usenixsecurity22/presentation/sullivan)

This USENIX paper refers to another document titled “Factoring RSA Keys with TLS Perfect Forward Secrecy” by Florian Weimer, dated September 2015. The discussion in the USENIX paper also refers to a document titled, “Memo on RSA signature generation in the presence of faults” by Arjen K. Lenstra, dates September 28 – October 28, 1996.

Although the research paper did not pinpoint the root cause of the issue in either silicon or software, it does offer a good recommendation for a preventive countermeasure in all Chinese Remainder Theorem (CRT RSA) signature calculations to mitigate the risk.

The following Marvell products could be subject to the vulnerability and could take advantage of the countermeasure:

- Liquid Security Devices
- Nitrox security processors and OCTEON™ general processors family

Marvell is implementing firmware improvements to include the countermeasure in all Liquid Security CRT RSA signature calculations as part of a software upgrade. If customers build their own devices and production software using either Nitrox or OCTEON processor crypto primitives to implement CRT optimization, then we recommend customers implement the countermeasure to validate the RSA signature before sending it per the USENIX research paper.

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