



Security Advisory

Published: May 31, 2022

CVE-2022-23960

In March 2022, researchers within the Systems and Network Security Group at Vrije Universiteit Amsterdam disclosed a new cache speculation vulnerability known as Branch History Injection (BHI), also known as Spectre-BHB. Spectre-BHB is similar to [Spectre v2](#), except that malicious code uses the shared branch history (stored in the CPU Branch History Buffer, or BHB) to influence mispredicted branches within the victim's own hardware context. Once that occurs, speculation caused by mispredicted branches can be used to cause cache allocation, which can then be used to infer information that should not be accessible. This vulnerability has been given the CVE number CVE-2022-23960 and affects the following Marvell family of products:

- CN106xx
- CNF105xx
- CNF95xx
- CN98xx
- CN96xx
- CN93xx
- CN92xx
- CN913x
- 88F80xx
- 88F70xx

A detailed description of this vulnerability and mitigations can be found on the [ARM Spectre-BHB page](#) with additional information in the [Spectre-BHB whitepaper](#) and [FAQ](#). For the latest information, refer to the [Spectre-BHB Knowledge Base Article](#).

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.