# CVE Detail – CVE-2019-6260

The ASPEED ast2400 and ast2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host (or from the network in unusual cases where the BMC console uart is attached to a serial concentrator). This CVE applies to the specific cases of iLPC2AHB bridge Pt I, iLPC2AHB bridge Pt II, PCIe VGA P2A bridge, DMA from/to arbitrary BMC memory via X-DMA, UART-based SoC Debug interface, LPC2AHB bridge, PCIe BMC P2A bridge, and Watchdog setup.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.7887

## CVSS Scoring

CVSS v3.0 Score: 9.8

Severity: CRITICAL

## Affected Products

* cpe:2.3:o:aspeedtech:ast2400\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:aspeedtech:ast2500\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:netapp:fas\/aff\_baseboard\_management\_controller:\*:\*:\*:\*:\*:\*:\*:\*