



CVE-2019-6260

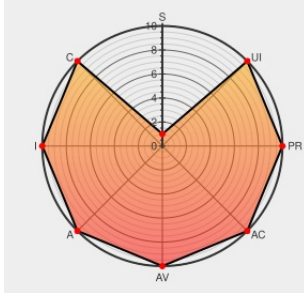
Published on: 01/22/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:02 PM UTC

CVE-2019-6260

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Ast2400](#) from [Aspeedtech](#) contain the following vulnerability:

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.

CVE-2019-6260 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Broadcom Inc. Connecting Everything	Third Party Advisory www.broadcom.com text/html	 CONFIRM www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2019-785
CVE-2019-6260 ASPEED BMC Vulnerability in NetApp Products NetApp Product Security	Patch Third Party Advisory security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20190314-0001/
CVE-2019-6260: Gaining control of BMC from the host processor Ramblings	Third Party Advisory www.flamingspork.com text/html	 MISC www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

A Test and Debug Tool for ASPEED BMC AHB Interfaces

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Aspeedtech	Ast2400	-	All	All	All
Hardware 	Aspeedtech	Ast2400	-	All	All	All
Operating System	Aspeedtech	Ast2400 Firmware	All	All	All	All
Operating System	Aspeedtech	Ast2400 Firmware	All	All	All	All
Hardware 	Aspeedtech	Ast2500	-	All	All	All
Hardware 	Aspeedtech	Ast2500	-	All	All	All
Operating System	Aspeedtech	Ast2500 Firmware	All	All	All	All
Operating System	Aspeedtech	Ast2500 Firmware	All	All	All	All
Application	Netapp	Fas/aff Baseboard Management Controller	All	All	All	All
Application	Netapp	Fas/aff Baseboard Management Controller	All	All	All	All
Application	Netapp	Fas/aff Baseboard Management Controller	All	All	All	All

cpe:2.3:h:aspeedtech:ast2400:-:*****:

cpe:2.3:h:aspeedtech:ast2400:-:*****:

cpe:2.3:o:aspeedtech:ast2400_firmware:*****:

cpe:2.3:o:aspeedtech:ast2400_firmware:*****:
cpe:2.3:h:aspeedtech:ast2500:-:*****:
cpe:2.3:h:aspeedtech:ast2500:-:*****:
cpe:2.3:o:aspeedtech:ast2500_firmware:*****:
cpe:2.3:o:aspeedtech:ast2500_firmware:*****:
cpe:2.3:a:netapp:fas/aff_baseboard_management_controller:*****:
cpe:2.3:a:netapp:fas\aff_baseboard_management_controller:*****:
cpe:2.3:a:netapp:fas\aff_baseboard_management_controller:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @mramboar	The AHB tracer is here: github.com/amboar/cve-201...	2021-04-16 09:06:49
 @mramboar	Save yourself from a bad day with an AST2600 with AHB command tracing. Now available over all the usual interfaces! github.com/amboar/cve-201...	2021-04-27 02:39:39
 @mramboar	Nice work by @oohal removing an awful work-around for SPI accesses over some of the the Aspeed AHB bridges github.com/amboar/cve-201...	2021-07-26 11:41:29

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)