

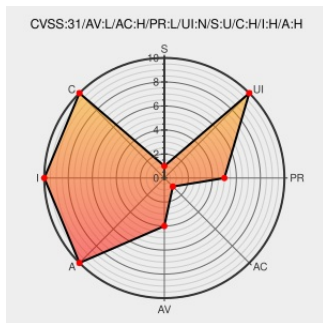


CVE-2021-34380

Published on: 06/30/2021 12:00:00 AM UTC

Last Modified on: 07/06/2021 03:23:00 PM UTC

CVE-2021-34380

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

Certain versions of [Jetson Agx Xavier 16gb](#) from [Nvidia](#) contain the following vulnerability:

Bootloader contains a vulnerability in NVIDIA MB2 where potential heap overflow might cause corruption of the heap metadata, which might lead to arbitrary code execution, denial of service, and information disclosure during secure boot.

CVE-2021-34380 has been assigned by [psirt@nvidia.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [NVIDIA](#) - **NVIDIA Jetson TX1, TX2 series, TX2 NX, AGX Xavier series, Xavier NX, Nano and Nano 2GB version All Jetson Linux versions prior to r32.5.1**

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

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

CVE References

Description	Tags	Link
Security Bulletin: NVIDIA Jetson AGX Xavier Series, Jetson Xavier NX, Jetson TX1, Jetson TX2 Series (including Jetson TX2	nvidia.custhelp.com text/html	CONFIRM nvidia.custhelp.com/app/answers/detail/a_id/5205

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Nvidia	Jetson Agx Xavier 16gb	-	All	All	All
Hardware 	Nvidia	Jetson Agx Xavier 32gb	-	All	All	All
Hardware 	Nvidia	Jetson Agx Xavier 8gb	-	All	All	All
Operating System	Nvidia	Jetson Linux	All	All	All	All
Hardware 	Nvidia	Jetson Tx2	-	All	All	All
Hardware 	Nvidia	Jetson Tx2i	-	All	All	All
Hardware 	Nvidia	Jetson Tx2 4gb	-	All	All	All
Hardware 	Nvidia	Jetson Tx2 Nx	-	All	All	All
Hardware 	Nvidia	Jetson Xavier Nx	-	All	All	All

cpe:2.3:h:nvidia:jetson_agx_xavier_16gb:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:nvidia:jetson_agx_xavier_32gb:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:nvidia:jetson_agx_xavier_8gb:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:o:nvidia:jetson_linux:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:nvidia:jetson_tx2:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:nvidia:jetson_tx2i:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:nvidia:jetson_tx2_4gb:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:nvidia:jetson_tx2_nx:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:nvidia:jetson_xavier_nx:-:~::~~::~~::~~::~~::~~::~~:::

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

 @CVEreport	CVE-2021-34380 : Bootloader contains a vulnerability in NVIDIA MB2 where potential heap overflow might cause corrup... twitter.com/i/web/status/1...	2021-06-30 10:30:26
 /r/netcve	CVE-2021-34380	2021-06-30 10:41:16

[< 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](#)