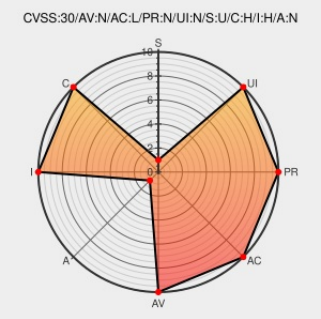
CVE-2019-5672

Published on: 04/11/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:59 PM UTC

CVE-2019-5672

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Jetson Tx1 from Nvidia contain the following vulnerability:

NVIDIA Jetson TX1 and TX2 contain a vulnerability in the Linux for Tegra (L4T) operating system (on all versions prior to R28.3) where the Secure Shell (SSH) keys provided in the sample rootfs are not replaced by unique host keys after sample rootsfs generation and flashing, which may lead to information disclosure.

CVE-2019-5672 has been assigned by psirt@nvidia.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **NVIDIA** - **Jetson TX1 and TX2** version **All versions prior to version R28.3**

CVSS3 Score: 9.1 - CRITICAL

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

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
Security Bulletin: NVIDIA Jetson TX1 and TX2 L4T - April	Vendor Advisory	CONFIRM

2019 | NVIDIA

nvidia.custhelp.com text/html nvidia.custhelp.com/app/answers/detail/a_id/4787

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nvidia	Jetson Tx1	All	All	All	All
Application	Nvidia	Jetson Tx1	All	All	All	All
Application	Nvidia	Jetson Tx2	All	All	All	All
Application	Nvidia	Jetson Tx2	All	All	All	All

cpe:2.3:a:nvidia:jetson_tx1:*:*:*:*:*:*:*:*:

cpe:2.3:a:nvidia:jetson_tx1:*:*:*:*:*:*:*:*:

cpe:2.3:a:nvidia:jetson_tx2:*:*:*:*:*:*:*:*:

cpe:2.3:a:nvidia:jetson_tx2:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→