



[Log In](#) | [Sign Up](#)

[NVIDIA Home](#) > [Support Home Page](#) > [Knowledgebase Home Page](#) > [Security Bulletin: NVIDIA Jetson and IGX Devices - March 2026](#)

# Security Bulletin: NVIDIA Jetson and IGX Devices - March 2026

Updated 03/30/2026 06:44 PM

NVIDIA has released a software update for NVIDIA® Jetson Linux.

To protect your system, download and install this software update from the APT server or [Jetson Download Center](#) page, [Jetson Linux Link](#) and [IGX Link](#).

Go to [NVIDIA Product Security](#).

## DETAILS

This section provides a summary of potential vulnerabilities that this security update addresses and their impact. Descriptions use [CWE™](#), and base scores and vectors use [CVSS v3.1](#) standards.

| CVE ID         | Description   | Vector  | Base Score | Severity | CWE                      | Impacts   |
|----------------|---|---|------------|----------|--------------------------|---|
| CVE-2026-24148 | NVIDIA Jetson for JetPack contains a vulnerability in the system initialization logic, where an unprivileged attacker could cause the initialization of a resource with an insecure default. A successful exploit of this vulnerability might lead to information disclosure of encrypted data, data tampering, and partial denial of service across devices sharing the same machine ID. | <a href="#">AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L</a> | 8.3        | High     | <a href="#">CWE-1188</a> | Data tampering, information disclosure, denial of service   |
| CVE-2026-24154 | NVIDIA Jetson Linux has vulnerability in initrd, where an unprivileged attacker with physical access could inject incorrect command line arguments. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, data tampering, and information disclosure.   | <a href="#">AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H</a> | 7.6        | High     | <a href="#">CWE-78</a>   | Code execution, escalation of privileges, denial of service, data tampering, information disclosure |
| CVE-2026-24153 | NVIDIA Jetson Linux has a vulnerability in initrd, where the nvlufs trusted application is not disabled. A successful exploit of this vulnerability might lead to information disclosure.   | <a href="#">AV:P/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N</a> | 5.2        | Medium   | <a href="#">CWE-501</a>  | Information disclosure  |

## SECURITY UPDATES

The following table lists the NVIDIA products affected, versions affected, and the updated version that includes this security update.

| CVE IDs Addressed | Affected Products                           | Platform or OS | Affected Versions            | Updated Version |
|-------------------|---|----------------|------------------------------|-----------------|
| CVE-2026-24148    | Jetson Xavier Series and Jetson Orin Series | Jetson Linux   | All versions prior to 35.6.4 | 35.6.4          |
|                   |   |                | All versions prior to 36.5   | 36.5            |



|                |  |      |      |
|----------------|--|------|------|
| CVE-2026-24154 |  | 38.2 | 38.4 |
|----------------|--|------|------|

### NOTES

To protect your system, download and install this software update from the APT server or [Jetson Download Center](#) page, [Jetson Linux Link](#) and [IGX Link](#).

### ACKNOWLEDGEMENTS

NVIDIA thanks the following for reporting their findings:

CVE-2026-24148: Ozgur Ogul Koca

CVE-2026-24153, CVE-2026-24154: th3\_h1tchh1ker

### GET THE MOST UP-TO-DATE PRODUCT SECURITY INFORMATION

Visit the [NVIDIA Product Security](#) page to

- Subscribe to security bulletin notifications
- See the current list of NVIDIA security bulletins
- Report a potential security issue in any NVIDIA supported product
- Learn more about the vulnerability management process followed by the NVIDIA Product Security Incident Response Team (PSIRT)

### REVISION HISTORY

| Revision | Date          | Description     |
|----------|---------------|-----------------|
| 1.0      | 31 March 2026 | Initial release |

### SUPPORT

If you have any questions about this security bulletin, contact [NVIDIA Support](#).

#### Disclaimer

ALL NVIDIA INFORMATION, DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, "MATERIALS") ARE BEING PROVIDED "AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR CONDITION OF TITLE, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT PERMITTED BY LAW.

Information is believed to be accurate and reliable at the time it is furnished. However, NVIDIA Corporation assumes no responsibility for the consequences of use of such information or for any infringement of patents or other rights of third parties that may result from its use. No license is granted by implication or otherwise under any patent or patent rights of NVIDIA Corporation. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. NVIDIA Corporation products are not authorized for use as critical components in life support devices or systems without express written approval of NVIDIA Corporation.



Chat online with one of our support agents

CHAT NOW

Contact Support for assistance

800.797.6530

ASK A QUESTION

