



# Incus does not verify combined fingerprint when downloading images from simplestreams servers

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-33542
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-26 23:16:20 UTC
<b>Updated</b>	2026-03-30 18:48:50 UTC
<b>Description</b>	Incus is a system container and virtual machine manager. Prior to version 6.23.0, a lack of validation of the image fingerprint

## Risk And Classification

**Primary CVSS:** v4.0 5.7 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:N/SC:L/SI:H/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000360000 probability, percentile 0.106790000 (date 2026-04-01)

**Problem Types:** CWE-295 | CWE-295 CWE-295: Improper Certificate Validation

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	5.7	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:N/SC:L/S
4.0	CNA	DECLARED	5.7	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:N/SC:L/S
3.1	nvd@nist.gov	Primary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

High

Availability

None

Sub Conf.

Low

Sub Integrity

High

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:N/SC:L/SI:H/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxcontainers	Incus	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CVE			2024-08-01	Linux

CNA

Lxc

Incus

affected < 6.23.0

Not specified

## References

Reference	Source	Link	Tags
github.com/lxc/incus/security/advisories/GHSA-p8mm-23gg-jc9r	security-advisories@github.com	github.com	Exploit, Mitigation, Vendor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

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](#)**