erofs: handle overlapped pclusters out of crafted images properly

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-47736
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-21 13:15:03 UTC
Updated	2026-04-11 13:16:34 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: erofs: handle overlapped pclusters out of crafted images p

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-667

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 8e6c8fa9f2e95c88a642521a5da19a8e31748846 c1172e65aad4b115392ea4c6e61e56e5b9b69df4 gi
CNA	Linux	Linux	affected 8e6c8fa9f2e95c88a642521a5da19a8e31748846 1bf7e414cac303c9aec1be67872e19be8b64980c git
CNA	Linux	Linux	affected 8e6c8fa9f2e95c88a642521a5da19a8e31748846 b9b30af0e86ffb485301ecd83b9129c9dfb7ebf8 git
CNA	Linux	Linux	affected 8e6c8fa9f2e95c88a642521a5da19a8e31748846 9cfa199bcbbbba31cbf97b2786f44f4464f3f29a git
CNA	Linux	Linux	affected 8e6c8fa9f2e95c88a642521a5da19a8e31748846 9e2f9d34dd12e6e5b244ec488bcebd0c2d566c50 gi
CNA	Linux	Linux	affected 5.13
CNA	Linux	Linux	unaffected 5.13 semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.72 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.13 6.10.* semver
CNA	Linux	Linux	unaffected 6.11.2 6.11.* semver
CNA	Linux	Linux	unaffected 6.12 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/9e2f9d34dd12e6e5b244ec488bcebd0c2d566c50	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/9cfa199bcbbbba31cbf97b2786f44f4464f3f29a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/c1172e65aad4b115392ea4c6e61e56e5b9b69df4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/b9b30af0e86ffb485301ecd83b9129c9dfb7ebf8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/1bf7e414cac303c9aec1be67872e19be8b64980c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report