ipv6: ioam: fix heap buffer overflow in __ioam6_fill_trace_data()

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

Summary

CVE	CVE-2026-43186
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:37 UTC
Updated	2026-05-11 20:40:56 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ipv6: ioam: fix heap buffer overflow in __ioam6_fill_trace_

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.001810000 probability, percentile 0.393470000 (date 2026-05-12)

Problem Types: CWE-787

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/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	F
CNA	Linux	Linux	affected 9ee11f0fff205b4b3df9750bff5e94f97c71b6a0 f4d9d4b8fd839719d564651671e24c62c545c23b git	N
CNA	Linux	Linux	affected 9ee11f0fff205b4b3df9750bff5e94f97c71b6a0 fb3c662fafebc5b9d74417ed1de8759f6bb72143 git	N
CNA	Linux	Linux	affected 9ee11f0fff205b4b3df9750bff5e94f97c71b6a0 632d233cf2e64a46865ae2c064ae3c9df7c8864f git	N
CNA	Linux	Linux	affected 9ee11f0fff205b4b3df9750bff5e94f97c71b6a0 0591d6509c2ff13f09ea2998434aba0c0472e978 git	N
CNA	Linux	Linux	affected 9ee11f0fff205b4b3df9750bff5e94f97c71b6a0 e90346a2f1e8917d5760a44a1f61c44e3b36d96b git	N
CNA	Linux	Linux	affected 9ee11f0fff205b4b3df9750bff5e94f97c71b6a0 ea3632aefc04205436868541638e26f4a74d5637 git	N
CNA	Linux	Linux	affected 9ee11f0fff205b4b3df9750bff5e94f97c71b6a0 6db8b56eed62baacaf37486e83378a72635c04cc git	N
CNA	Linux	Linux	affected 5.15	N
CNA	Linux	Linux	unaffected 5.15 semver	N
CNA	Linux	Linux	unaffected 5.15.202 5.15.* semver	N
CNA	Linux	Linux	unaffected 6.1.165 6.1.* semver	N
CNA	Linux	Linux	unaffected 6.6.128 6.6.* semver	N
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver	N
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver	N
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver	N
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix	N

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/0591d6509c2ff13f09ea2998434aba0c0472e978	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/6db8b56eed62baacaf37486e83378a72635c04cc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/632d233cf2e64a46865ae2c064ae3c9df7c8864f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/e90346a2f1e8917d5760a44a1f61c44e3b36d96b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/fb3c662fafebc5b9d74417ed1de8759f6bb72143	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch

git.kernel.org/stable/c/f4d9d4b8fd839719d564651671e24c62c545c23b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/ea3632aefc0420543686854 1638e26f4a74d5637	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

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