Bluetooth: hci_conn: fix potential UAF in set_cig_params_sync

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

Summary

CVE	CVE-2026-43019
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 15:16:46 UTC
Updated	2026-05-03 07:16:22 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_conn: fix potential UAF in set_cig_params_

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000180000 probability, percentile 0.046600000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected a091289218202bc09d9b9caa8afcde1018584aec 66d432e9b45bae7881ffcdb12cd8fd0bf254ef02 git
CNA	Linux	Linux	affected a091289218202bc09d9b9caa8afcde1018584aec 7d568fede8eac91161a60b710aa920abe9b0fb9f git
CNA	Linux	Linux	affected a091289218202bc09d9b9caa8afcde1018584aec bad65b4b0a96139f023eadc28a33125963208449 g
CNA	Linux	Linux	affected a091289218202bc09d9b9caa8afcde1018584aec a2639a7f0f5bf7d73f337f8f077c19415c62ed2c git
CNA	Linux	Linux	affected 3a273cd0f47dd672d37736e623849374f9ab9ce9 git
CNA	Linux	Linux	affected d8570c4c3f2a3e51b3c8b5e6ec898364c5c03062 git
CNA	Linux	Linux	affected 6.6
CNA	Linux	Linux	unaffected 6.6 semver
CNA	Linux	Linux	unaffected 6.12.81 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.22 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.12 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/a2639a7f0f5bf7d73f337f8f077c19415c62ed2c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/66d432e9b45bae7881ffcdb12cd8fd0bf254ef02	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/bad65b4b0a96139f023eadc28a33125963208449	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/7d568fede8eac91161a60b710aa920abe9b0fb9f	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