Bluetooth: hci_event: fix potential UAF in hci_le_remote_conn_param_req_evt

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

Summary

CVE	CVE-2026-43018
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 15:16:45 UTC
Updated	2026-05-03 07:16:22 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_event: fix potential UAF in hci_le_remote_c

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000240000 probability, percentile 0.068220000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	8.8	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector
Adjacent

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 95118dd4edfec950898a00180c6f998df0a6406d 59eecf0ffde15670e6a5e10c47be67f73d843b20 git
CNA	Linux	Linux	affected 95118dd4edfec950898a00180c6f998df0a6406d 5fb69e1eeea9d6cba80517e9f058b56b34bc3a81 git
CNA	Linux	Linux	affected 95118dd4edfec950898a00180c6f998df0a6406d 7cadb03be37e761130edb153544fe0770a842b19 git
CNA	Linux	Linux	affected 95118dd4edfec950898a00180c6f998df0a6406d 1d0bdbfe3e91c11f0a704c52443a9446a10d699c git
CNA	Linux	Linux	affected 95118dd4edfec950898a00180c6f998df0a6406d ea3cd36d7382d5f8309df04c275d20df139ed42c git
CNA	Linux	Linux	affected 95118dd4edfec950898a00180c6f998df0a6406d b255531b27da336571411248c2a72a350662bd09 gi
CNA	Linux	Linux	affected 5.17
CNA	Linux	Linux	unaffected 5.17 semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.134 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/7cadb03be37e761130edb153544fe0770a842b19	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/5fb69e1eeea9d6cba80517e9f058b56b34bc3a81	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/59eecf0ffde15670e6a5e10c47be67f73d843b20	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/b255531b27da336571411248c2a72a350662bd09	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1d0bdbfe3e91c11f0a704c52443a9446a10d699c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ea3cd36d7382d5f8309df04c275d20df139ed42c	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.