HID: i2c-hid: fix potential buffer overflow in i2c_hid_get_report()

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

Summary

CVE	CVE-2026-23178
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-14 17:15:55 UTC
Updated	2026-04-03 14:16:25 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: HID: i2c-hid: fix potential buffer overflow in i2c_hid_get_re

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 0.046610000 (date 2026-04-07)

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 85df713377ddc0482071c3e6b64c37bd1e48f1f1 f9c9ad89d845f88a1509e9d672f65d234425fde9 git
CNA	Linux	Linux	affected 85df713377ddc0482071c3e6b64c37bd1e48f1f1 cff3f619fd1cb40cdd89971df9001f075613d219 git
CNA	Linux	Linux	affected 85df713377ddc0482071c3e6b64c37bd1e48f1f1 786ec171788bdf9dda38789163f1b1fbb47f2d1e git
CNA	Linux	Linux	affected 85df713377ddc0482071c3e6b64c37bd1e48f1f1 2124279f1f8c32c1646ce98e75a1a39b23b7db76 git
CNA	Linux	Linux	affected 85df713377ddc0482071c3e6b64c37bd1e48f1f1 2497ff38c530b1af0df5130ca9f5ab22c5e92f29 git
CNA	Linux	Linux	affected 5.18
CNA	Linux	Linux	unaffected 5.18 semver
CNA	Linux	Linux	unaffected 6.1.163 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.124 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.70 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.10 6.18.* semver
CNA	Linux	Linux	unaffected 6.19 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/2497ff38c530b1af0df5130ca9f5ab22c5e92f29	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2124279f1f8c32c1646ce98e75a1a39b23b7db76	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f9c9ad89d845f88a1509e9d672f65d234425fde9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/786ec171788bdf9dda38789163f1b1fbb47f2d1e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/cff3f619fd1cb40cdd89971df9001f075613d219	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
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.

Free CVE JSON API cve.report/api

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