



# HID: logitech-dj: Fix memory leak in logi\_dj\_recv\_switch\_to\_dj\_mode()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2024-40934
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-07-12 13:15:15 UTC
<b>Updated</b>	2026-05-12 12:16:59 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: HID: logitech-dj: Fix memory leak in logi_dj_recv_switch_t

## 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-401

## 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 cf48a7ba5c095f76bb9c1951f120fa04844242
CNA	Linux	Linux	affected e38a6f12685d8a2189b72078f6254b069ff84f
CNA	Linux	Linux	affected 4fb28379b3c735398b252a979c991b340baa
CNA	Linux	Linux	affected 6e59609541514d2ed3472f5bc999c55bdb61
CNA	Linux	Linux	affected 6f20d3261265885f6a6be4cda49d70197287f
CNA	Linux	Linux	affected 6f20d3261265885f6a6be4cda49d70197287f
CNA	Linux	Linux	affected 6f20d3261265885f6a6be4cda49d70197287f
CNA	Linux	Linux	affected 144becd79c196f02143ca71fc10766bd0cc66
CNA	Linux	Linux	affected 00ab92481d3a40a5ad323df4c518068f66ce4
CNA	Linux	Linux	affected 6.6
CNA	Linux	Linux	unaffected 6.6 semver
CNA	Linux	Linux	unaffected 5.4.279 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.221 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.162 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.95 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.35 6.6.* semver
CNA	Linux	Linux	unaffected 6.9.6 6.9.* semver
CNA	Linux	Linux	unaffected 6.10 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	unaffected * custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	unaffected * custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

## References

Reference	Source	Link
git.kernel.org/stable/c/a0503757947f2e46e59c1962326b53b3208c8213	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/caa9c9acb93db7ad7b74b157cf101579bac9596d	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.co</a>
git.kernel.org/stable/c/789c99a1d7d2c8f6096d75fc2930505840ec9ea0	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>

<a href="https://git.kernel.org/stable/c/15122dc140d82c51c216535c57b044c4587aae45">git.kernel.org/stable/c/15122dc140d82c51c216535c57b044c4587aae45</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/ce3af2ee95170b7d9e15fff6e500d67deab1e7b3">git.kernel.org/stable/c/ce3af2ee95170b7d9e15fff6e500d67deab1e7b3</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/1df2ead5dfad5f8f92467bd94889392d53100b98">git.kernel.org/stable/c/1df2ead5dfad5f8f92467bd94889392d53100b98</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-355557.html">cert-portal.siemens.com/productcert/html/ssa-355557.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.co</a>
<a href="https://lists.debian.org/debian-lts-announce/2025/01/msg00001.html">lists.debian.org/debian-lts-announce/2025/01/msg00001.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
<a href="https://git.kernel.org/stable/c/f677ca8cfefee2a729ca315f660cd4868abdf8de">git.kernel.org/stable/c/f677ca8cfefee2a729ca315f660cd4868abdf8de</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)