



# Libinput: libinput: information disclosure via dangling pointer in lua plugin handling

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

## Summary

<b>CVE</b>	CVE-2026-35094
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-01 14:16:57 UTC
<b>Updated</b>	2026-04-01 14:23:37 UTC
<b>Description</b>	A flaw was found in libinput. An attacker capable of deploying a Lua plugin file in specific system directories can exploit a d

## Risk And Classification

**Primary CVSS:** v3.1 3.3 LOW from secalert@redhat.com

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

**Problem Types:** CWE-825 | CWE-825 Expired Pointer Dereference

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	3.3	LOW	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	3.3	LOW	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat Enterprise Linux 10</a>	Not specified	Not specified
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat Enterprise Linux 7</a>	Not specified	Not specified
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat Enterprise Linux 8</a>	Not specified	Not specified
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat Enterprise Linux 9</a>	Not specified	Not specified

### References

Reference	Source	Link	Tags
<a href="https://access.redhat.com/security/cve/CVE-2026-35094">access.redhat.com/security/cve/CVE-2026-35094</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://access.redhat.com">access.redhat.com</a>	
<a href="https://gitlab.freedesktop.org/libinput/libinput/-/work_items/1272">gitlab.freedesktop.org/libinput/libinput/-/work_items/1272</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://gitlab.freedesktop.org">gitlab.freedesktop.org</a>	
<a href="https://bugzilla.redhat.com/show_bug.cgi">bugzilla.redhat.com/show_bug.cgi</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Red Hat would like to thank Koen Tange ([monokles.eu](https://monokles.eu)) for reporting this issue. (en)

### Additional Advisory Data

Source	Time	Event
CNA	2026-04-01T13:36:01.001Z	Reported to Red Hat.
CNA	2026-04-01T00:00:00.000Z	Made public.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

