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

MITRE | NVD | CVE.ORG | Print: PDF

Summary

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

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	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified

References

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

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Koen Tange (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 and Source URL Uptime Status status.cve.report