VDB-354671 · CVE-2026-5342 · ISSUE 795

LIBRAW UP TO 0.22.0 TIFF/NEF DECODERS_LIBRAW.CPP NIKON_LOAD_PADDED_PACKED_RAW LOAD_FLAGS/RAW_WIDTH OUT-OF-BOUNDS

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.8	$0-$5k	0.97

Summary

A vulnerability identified as problematic has been detected in LibRaw up to 0.22.0. This impacts the function `LibRaw::nikon_load_padded_packed_raw` of the file *src/decoders/decoders_libraw.cpp* of the component *TIFF/NEF*. The manipulation of the argument *load_flags/raw_width* leads to out-of-bounds. This vulnerability is documented as CVE-2026-5342. The attack can be initiated remotely. Additionally, an exploit exists. You should upgrade the affected component.

Details

A vulnerability was found in LibRaw up to 0.22.0. It has been rated as problematic. This issue affects the function `LibRaw::nikon_load_padded_packed_raw` of the file *src/decoders/decoders_libraw.cpp* of the component *TIFF/NEF*. The manipulation of the argument `load_flags/raw_width` with an unknown input leads to a out-of-bounds vulnerability. Using CWE to declare the problem leads to CWE-125. The product reads data past the end, or before the beginning, of the intended buffer. Impacted is availability.

It is possible to read the advisory at github.com. The identification of this vulnerability is CVE-2026-5342. The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. Technical details as well as a public exploit are known.

The exploit is available at github.com. It is declared as proof-of-concept.

Upgrading to version 0.22.1 eliminates this vulnerability. The upgrade is hosted for download at github.com. Applying the patch b8397cd45657b84e88bd1202528d1764265f185c is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.

The vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-18344). Entries connected to this vulnerability are available at VDB-120461, VDB-147179, VDB-288215 and VDB-354650.

Product

Type

- Image Processing Software

Name

- LibRaw

Version

- 0.1
- 0.2
- 0.3
- 0.4
- 0.5
- 0.6
- 0.7
- 0.8
- 0.9
- 0.10
- 0.11
- 0.12
- 0.13
- 0.14
- 0.15

License

- open-source

Website

- Product: https://github.com/LibRaw/LibRaw/

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 5.3
VulDB Meta Temp Score: 4.8

VulDB Base Score: 5.3
VulDB Temp Score: 4.8
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Out-of-bounds
CWE: CWE-125 / CWE-119
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public

Status: Proof-of-Concept
Download: 🔒

EPSS Score: 🔒
EPSS Percentile: 🔒

Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: Upgrade
Status: 🔍

0-Day Time: 🔒

Upgrade: LibRaw 0.22.1
Patch: b8397cd45657b84e88bd1202528d1764265f185c

Timeline

04/01/2026		Advisory disclosed
04/01/2026	+0 days	VulDB entry created
04/07/2026	+6 days	VulDB entry last update

Sources

Product: github.com

Advisory: 795
Status: Confirmed
Confirmation: 🔒

CVE: CVE-2026-5342 (🔒)

GCVE (CVE): GCVE-0-2026-5342
GCVE (VulDB): GCVE-100-354671
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/01/2026 04:57 PM
Updated: 04/07/2026 01:31 PM
Changes: 04/01/2026 04:57 PM (63), 04/02/2026 07:59 PM (1), 04/07/2026 01:31 PM (1)
Complete: 🔍
Submitter: biniam
Cache ID: 13:CB9:179

Submit

Accepted

- Submit #781223: LibRaw 0.22.0 Out-of-Bounds Read (by biniam)

Discussion

No comments yet. Languages: en.

Please log in to comment.

© 1997-2026 vuldb.com · cc by-nc-sa

v20.2.1