



VDB-354650 · CVE-2026-5318 · ISSUE 794

LIBRAW UP TO 0.22.0 JPEG DHT PARSER LOSSLESSJPEG.CPP HUFFTABLE::INITVAL BITS[] OUT-OF-BOUNDS WRITE

CVSS Meta Temp Score ⓘ

3.9

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

0.86

Summary

A vulnerability, which was classified as **critical**, was found in **LibRaw up to 0.22.0**. Affected is the function `HuffTable::initval` of the file `src/decompressors/losslessjpeg.cpp` of the component **JPEG DHT Parser**. Such manipulation of the argument `bits[]` leads to out-of-bounds write. This vulnerability is referenced as **CVE-2026-5318**. It is possible to launch the attack remotely. Furthermore, an exploit is available. You should upgrade the affected component.

Details

A vulnerability was found in **LibRaw up to 0.22.0** and classified as **problematic**. Affected by this issue is the function `HuffTable::initval` of the file `src/decompressors/losslessjpeg.cpp` of the component **JPEG DHT Parser**. The manipulation of the argument `bits[]` with an unknown input leads to a out-of-bounds write vulnerability. Using CWE to declare the problem leads to **CWE-787**. The product writes data past the end, or before the beginning, of the intended buffer. Impacted is availability.

The advisory is available at github.com. This vulnerability is handled as **CVE-2026-5318**. The exploitation is known to be easy. The attack may be launched remotely. No form of authentication is required for exploitation. Successful exploitation requires user interaction by the victim. 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 `a6734e867b19d75367c05f872ac26322464e3995` 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 databases at CNNVD (**CNNVD-202604-466**) and EUVD (**EUVD-2026-18116**). Similar entries are available at **VDB-115045**, **VDB-115886**, **VDB-212004** and **VDB-212005**.

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: 4.3

VulDB Meta Temp Score: 3.9

VulDB Base Score: 4.3

VulDB Temp Score: 3.9

VulDB Vector: 

VulDB Reliability: 

CVSSv2

VulDB Base Score: 

VulDB Temp Score: 

VulDB Reliability: 

Exploiting

Class: Out-of-bounds write

CWE: [CWE-787](#) / [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: [a6734e867b19d75367c05f872ac26322464e3995](#)

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: [794](#)

Status: Confirmed

Confirmation:

CVE: [CVE-2026-5318](#) ()

GCVE (CVE): [GCVE-0-2026-5318](#)

GCVE (VulDB): [GCVE-100-354650](#)

EUVD: 

CNNVD: [CNNVD-202604-466](#) - Libraw 缓冲区错误漏洞

scip Labs: <https://www.scip.ch/en/?labs.20161013>

See also: 

Entry

Created: 04/01/2026 02:48 PM

Updated: 04/07/2026 01:31 PM

Changes: 04/01/2026 02:48 PM (63), 04/01/2026 04:18 PM (1), 04/02/2026 09:42 AM (1), 04/03/2026 10:54 PM (6), 04/04/2026 11:53 PM (1), 04/06/2026 10:48 AM (1), 04/07/2026 07:46 AM (1), 04/07/2026 01:31 PM (1)

Complete: 

Submitter: biniam

Cache ID: 52:03C:179

Submit

Accepted

- [Submit #780538](#): LibRaw 0.22.0 Out-of-bounds Write (by biniam)

Discussion

No comments yet. Languages: en.

Please log in to comment.